明　細　書

信号処理システム

技術分野

この発明は、例えばパーソナルコンピュータと接続されたドライブによってディスクメディア例えばＤＶＤ (Digital Versatile Disc)規格のディスクにコンテンツを記録し、また、ディスクメディアからコンテンツを再生する場合に適用される信号処理システム、記録再生装置、記録方法、記録方法のプログラム並びに記録媒体に関する。

背景技術

近年開発されたＤＶＤ等の記録媒体では、１枚の媒体に例えば映画１本分の大量のデータをデジタル情報として記録することが可能である。このように、大量の映像情報等をデジタル情報として記録することが可能になると、不正コピーを防止して著作権者の保護を図ることが益々重要になってくる。

例えば、ＤＶＤ－Videoでは、ＣＳＳ(Content Scramble System)と呼ばれる著作権保護技術が採用されている。ＤＶＤに関する著作権保護の方法に関しては、下記の文献１および文献２説明されている。

（文献１）

「２部知的財産権保護　ソフトウェア復号のカギを握る不正コピー防止技術にメド」，日経エレクトロニクス 1997.8.18,p.110-119

（文献２）

山田，「ＤＶＤを起点に著作権保護空間を広げる」，日経エレクトロニ

クス 2001.8.13,p.143-153

第１図は、これらの文献に説明されているＣＳＳ方式の概要を示す。この方式の場合には、３つの暗号化鍵データが使用される。３つの暗号化鍵データは、ＣＳＳ鍵発行センターが発行するマスターキーと、著作権者等が決めるディスクキーおよびタイトルキーである。マスターキーは、秘密とされ、メーカー毎に異なる固定の値の鍵であり、ディスクキーは、ディスク毎に異なる値の鍵である。何れのマスターキーでも復号できるようなディスクキーのセットが作成され、そのセットがディスクに格納される。ディスクキーをディスクに格納する場合に暗号化されており、セキュアドディスクキーと呼ばれる。

ビデオデータ、オーディオデータなどのコンテンツデータを圧縮したＭＰＥＧ(Moving Picture coding Experts Group)データ１に対して、そのコンテンツに割当てられた暗号化鍵であるタイトルキー２を用意する。さらに、１枚毎のディスクに割当てられた暗号化鍵であるディスクキー３を用意する。そして、暗号化の管理を行う鍵発行センター４では、そのセンター４が管理するマスタキー５を使用して、ディスクキー３を暗号化回路（以下、適宜エンクリプタと称する）６によって暗号化し、さらにディスクキー３を使用してタイトルキー２をエンクリプタ７によって暗号化する。そして、ＭＰＥＧデータ１に対してタイトルキー２によってスクランブラ８で暗号化する。

暗号化されたコンテンツデータ（以下、スクランブルドＭＰＥＧデータまたはスクランブルドコンテンツと適宜称する）９と、暗号化されたディスクキー（以下、セキュアドディスクキーと適宜称する）１０と、暗号化されたタイトルキー（以下、暗号化タイトルキーと適宜称する）１１とがＤＶＤ－Videoディスク製造時にＤＶＤ－Videoディスク１２に記録される。セキュアドディスクキーがディスク１２のリードインエリ

アの所定の位置に記録され、暗号化タイトルキーがセクタ構造化されたコンテンツデータの各セクタに記録される。これらのセキュアドディスクキーおよび暗号化タイトルキーは、著作権保護システム用の鍵情報であり、両者をまとめてＣＳＳキーと称する。

第２図に示すように、ＤＶＤプレイヤーによってＤＶＤ－Videoディスク１２が再生され、スクランブルドＭＰＥＧデータ９、セキュアドディスクキー１０および暗号化タイトルキー１１が再生され、ＤＶＤプレイヤー２１に読み込まれる。ＤＶＤプレイヤー２１では、マスターキー２２を使用して暗号化の復号回路（以下、適宜デクリプタと称する）２３によってディスクキーを復号し、復号したディスクキーを使用してデクリプタ２４によってタイトルキーを復号し、復号したタイトルキーを使用してデスクランブラ２５によってＭＰＥＧデータを復号する。ＭＰＥＧデコーダ２６によってオーディオ／ビジュアルデータ２７が復号される。

第３図は、ディスク再生時にプレイヤーが最初に読み取り出す領域であるリードインエリアのデータ構成を示す。リードインエリアは、物理的なセクタ番号が０ｈ（ｈは１６進数表記であることを示す記号：以下同じ）から３００００ｈのセクタまで使用され、最初に全ての値が０のエリアが配置され、その後に参照用コードが配置され、再度全ての値が０のエリアが配置され、その後にコントロールデータエリアが設けられている。その後、さらに全ての値が０のエリアがあり、セクタ番号３０００ｈからコンテンツデータが記録されるメインデータエリアとなる。

コントロールデータエリアは、最初の１セクタ（セクタ０）に物理フォーマット情報が配置され、次の１セクタ（セクタ１）にディスク製造情報が配置され、次の１４セクタ（セクタ２～１５）にコンテンツ供給者の情報が配置される。このセクタ０からセクタ１５までの１６セクタ

の情報が、コントロールデータエリアに繰り返し配置される。そして、コンテント・プロバイダー・インフォメーション（コンテンツ供給者の情報）が配置される区間に、そのディスクに特有のセキュアドディスクキーが配置される。

また、タイトルキーが記録される構造について、第４図に示すセクタ構造例に基づいて説明すると、コンテンツデータなどのメインデータが記録されるそれぞれのセクタは、２０６４バイトで構成される。この２０６４バイトの内の先頭の４バイトがセクタ番号などを示すＩＤデータとされ、続いた２バイトがＩＤデータエラー検出用データＩＥＤとされる。さらに次の６バイトがコピー管理用データＲＳＶとされ、このコピー管理用データＲＳＶの中に暗号化タイトルキーが配置される。そして、コピー管理用データに続いた２０４８（２Ｋ）バイトがコンテンツデータなどが記録されるメインデータの記録エリアとされる。さらに、最後の４バイトには、このセクタ全体のエラー検出用データＥＤＣが配置される。

このようにディスクキーとタイトルキーを使用して暗号化されてデータが格納されるディスクは、基本的に再生専用のディスクであるが、ＤＶＤ規格の中には、記録が可能な規格のディスクも存在する。例えば、ＤＶＤ－ＲＷ／－Ｒ規格のディスク、ＤＶＤ＋ＲＷ／＋Ｒ規格のディスクは、データの記録が可能であり、いわゆるビットバイビットコピー(bit by bit copy) と称される他の媒体から再生したデジタルデータを、そのまま別の媒体に記録させる処理を行って、ＤＶＤ－Videoから読出したデータを、これらの規格のディスクにそのまま記録させることで、ＤＶＤ－Videoディスクのビデオデータなどのコンテンツデータのコピーを不正に作成することができる。しかしながら、上述したディスクキーとタイトルキーが用意されることで、不正にコピーされたビデオデー

タなどのコンテンツデータが復号できないようになされる。

この不正にコピーされたディスクでは、暗号化からの正しい復号ができない点について、第５図を参照して説明する。まず、セキュアドディスクキーと暗号化タイトルキーとが上述した配置で記録されたＤＶＤ－Videoのディスク Ｄａを用意して、そのディスクＤａをユーザが再生する。プレイヤー内では、そのディスクの最内周部のリードインエリアからセキュアドディスクキーが得られ、コンテンツデータが記録されたセクタからは、暗号化タイトルキーが得られる。セキュアドディスクキーがマスターキーによって復号され、暗号化タイトルキーがディスクキーによって復号される。タイトルキーによって、スクランブルドＭＰＥＧデータが復号され、オーディオ／ビジュアルデータが得られる。

このＤＶＤ－Videoのディスク Ｄａに記録されたコンテンツデータをＤＶＤ－ＲＷ／－Ｒ規格のディスクＤｂに、ビットバイビットコピーで記録させることをユーザが実行したとする。ここで、ディスクＤｂは、リードインエリアの一部がディスク製造時にピットで書込み済みのエリアとしてあり、その書込み済みのエリアに、そのディスクＤｂに割当てられたディスクキー又は無効なキーが予め書き込んである。

したがって、ディスクＤｂのデータ記録可能エリアに、ＤＶＤ－Videoのディスク Ｄａから読出したコンテンツデータをそのまま記録させたＤＶＤ－Ｒ／ＲＷ規格のディスクＤｂ’をユーザが制作した場合、ディスクＤｂ’は、元のディスクＤａとはディスクキーが異なっている。ディスクキーが元のディスクＤａとは異なるために、コピーされたディスクＤｂ’をユーザが再生しようとしても、プレイヤーでは、正しく復号することができず、結果的に不正コピーが防止されることになる。

なお、ここでは主としてＤＶＤ－Videoのディスクに適用されるＣＳＳ方式の場合について説明したが、ＤＶＤオーディオのディスクなどに

適用されるスクランブル方式であるＣＰＰＭ(Content Protection for Pre-Recorded)方式の場合にも、基本的な原理は同じである。

第６図は、ＣＳＳ方式で記録されたＲＯＭディスク例えばＤＶＤ－Videoディスクを再生するＰＣとドライブでのディスクキーとタイトルキーの取り出し方、およびスクランブルデータのデスクランブルの方法を示すものである。第６図において、参照符号３１がＣＳＳで記録されたＤＶＤ－Videoディスクを再生する再生装置としてのＤＶＤドライブを示す。参照符号４１がデータ処理装置としてのＰＣを示す。ＰＣ４１に対してＤＶＤプレイヤーアプリケーションソフトウェアがインストールされる。

ＤＶＤドライブ３１とＰＣ４１との間が標準的なインターフェースで接続されている。インターフェースは、ＡＴＡＰＩ(AT Attachment with Packet Interface)，ＳＣＳＩ(Small Computer System Interface)，ＵＳＢ(Universal Serial Bus)，ＩＥＥＥ(Institute of Electrical and Electronics Engineers)１３９４等である。

ＤＶＤドライブ３１には、認証部３２、バスエンクリプタ３３および３４が備えられている。ＰＣ４１には、認証部４２、バスエンクリプタ４３および４４が備えられている。認証部３２および認証部４２は、相互認証を行い、認証動作の度に異なるセッションキー（バスキーとも呼ばれる）Ｋｓを生成する。また、ＰＣ４１には、マスターキー４５、デクリプタ４６および４７、デスクランブラ４８が備えられ、デスクランブラ４８から得られたＭＰＥＧデータがＭＰＥＧデコーダ４９で復号されることによってオーディオ／ビジュアルデータ５０が得られる。

なお、認証動作は、電源のＯＮ後のディスク検出時並びにディスクの交換時には、必ず行われる。また、記録ボタンを押して記録動作を行う場合、並びに再生ボタンを押して再生動作を行う場合に、認証動作を行

うようにしても良い。一例として、記録ボタンまたは再生ボタンを押した時に、認証がなされる。

ＤＶＤ－Videoディスクから得られたスクランブルドＭＰＥＧデータ９、セキュアドディスクキーが１０、暗号化タイトルキー１１がＤＶＤドライブ３１に読み込まれる。コンテンツデータが記録されたセクタからは、暗号化タイトルキーが得られる。セキュアドディスクキーがマスターキーによって復号され、暗号化タイトルキーがディスクキーによって復号される。タイトルキーによって、スクランブルドＭＰＥＧデータが復号され、オーディオ／ビジュアルデータが得られる。

第７図は、第６図に示す現行のシステムにおいて、ＤＶＤドライブ３１とＰＣ４１との間の信号の授受の手順を示す。ＰＣ４１がＤＶＤドライブ３１に対してコマンドを送り、ＤＶＤドライブ３１がコマンドに応答した動作を行う。ＤＶＤ－Videoディスクの挿入等でシーケンスが開始し、最初に認証シーケンスＡＫＥ(Authentication and Key Exchange)（ステップＳ１）がなされる。相互認証が成立すると、セッションキーＫｓをＤＶＤドライブ３１とＰＣ４１が共有する。認証が成立しなかった場合では、処理が中断する。

次に、ＰＣ４１からの要求に応じてＤＶＤ－Videoディスク１２上のコンテンツデータゾーンがシークされ、読み出される（ステップＳ２）。次のステップＳ３において、セキュアドディスクキーをＰＣ４１がドライブ３１に対して要求し、ドライブ３１がＤＶＤ－Videoディスク１２からセキュアドディスクキーを読み取る（ステップＳ４，Ｓ５）。セキュアドディスクキーがセッションキーＫｓを使用してバスエンクリプタ３３によって暗号化される。Ｋｓで暗号化されたセキュアドディスクキーがドライブ３１からＰＣ４１に戻される（ステップＳ６）。

次に、暗号化タイトルキーおよびコピー世代管理情報ＣＧＭＳ(Copy

Generation Managemrnt System)をＰＣ４１がドライブ３１に対して要求し（ステップＳ７）、ドライブ３１がＤＶＤ－Videoディスク１２から暗号化タイトルキーおよびＣＧＭＳを読み取る（ステップＳ８，Ｓ９）。暗号化タイトルキーおよびＣＧＭＳがセッションキーＫｓを使用してバスエンクリプタ３４によって暗号化される。Ｋｓで暗号化された暗号化タイトルキーおよびＣＧＭＳがドライブ３１からＰＣ４１に戻される（ステップＳ１０）。

次に、スクランブルドコンテンツ（スクランブルドＭＰＥＧデータと同一の意味である）をＰＣ４１がドライブ３１に対して要求し（ステップＳ１１）、ドライブ３１がＤＶＤ－Videoディスク１２からスクランブルドコンテンツを読み取る（ステップＳ１２，Ｓ１３）。スクランブルドコンテンツがドライブ３１からＰＣ４１に戻される（ステップＳ１４）。

上述したＣＳＳ方式は、ＤＶＤ－ＲＯＭメディアに対する適用のみが認可されており、ＤＶＤ－Ｒ、ＤＶＤ－ＲＷ、ＤＶＤ＋Ｒ、ＤＶＤ＋ＲＷ等の記録型ＤＶＤでのＣＳＳ方式の利用がＣＳＳ契約によって禁止されている。したがって、ＣＳＳ方式で著作権保護されたＤＶＤ－Videoの内容を記録型ＤＶＤへのまるごとコピー（ビットバイビットコピー）することは、ＣＳＳ契約上では、認められた行為ではない。

しかしながら、ＣＳＳの暗号方式が破られる事態が発生した。ＣＳＳの暗号化を解除してＤＶＤ－Videoの内容を簡単にハードディスクにコピーすることを可能とする「ＤｅＣＳＳ」と呼ばれるソフトウェアがインターネット上で配布された。「ＤｅＣＳＳ」が出現した背景には、本来耐タンパー化が義務付けられているはずのＣＳＳ復号用の鍵データを耐タンパー化しないまま設計された再生ソフトウェアがリバースエンジニアされて鍵データが解読されたことによって、連鎖的にＣＳＳアルゴ

リズム全体が解読された経緯がある。

ＣＳＳの後に、ＤＶＤ－Audio等のＤＶＤ－ＲＯＭの著作権保護技術であるＣＰＰＭ(Content Protection for Pre-Recorded Media)、並びに記録型ＤＶＤ、メモリカードに関する著作権保護技術ＣＰＲＭ(Content Protection for Recordable Media) が提案されている。これらの方式は、コンテンツの暗号化や管理情報の格納等に問題が生じたときに、システムを更新でき、また、データをまるごとコピーしても再生を制限できる特徴を有している。すなわち、ＣＰＲＭは、ビットバイビットコピーを禁止するため、リードインエリアの鍵情報を記録するエリアを予め記録済みとしている。ＣＰＲＭは、ライセンス管理者である米4C Entity,LLCが配布する下記の資料（文献３）に説明されている。

（文献３）

"Content Protection for Recordable Media Specification DVD Book"、インターネット＜ＵＲＬ：http://www.4Centity.com/＞

しかしながら、市場に既に大量に供給されたＤＶＤプレイヤーは、後から規格化されたＣＰＲＭへ対応しておらず、また、ＣＰＲＭ規格化後のＤＶＤプレイヤーもコスト的な理由からＣＰＲＭへ対応しないものが殆どである。したがって、既存のＤＶＤ－Videoプレイヤーとの互換性を考慮すると、ＣＰＲＭを採用しにくい。一方、ＢＳディジタル放送および地上波デジタル放送の実用化と共に、放送コンテンツの著作権の保護のために、放送の暗号化記録に対する必要性が増大している。

「ＤｅＣＳＳ」が出現してきた状況において、コンテンツの著作権を保護する他の方法として、予めオーディオ／ビジュアルデータに電子透かし情報を埋め込んでおくことが考えられる。電子透かし情報は、コピー後でも保存されるので、再生時に電子透かし情報を検出して再生を禁止することが可能である。

しかしながら、電子透かし情報を埋め込む方法は、いくつかの問題があり、実際に行うことが難しい。すなわち、オーディオ／ビジュアル情報の単位より小さい単位でのランダムアクセスが可能なこと、ＡＴＡＰＩという一つのチャンネルを介して読み出しデータと書き込みデータが流れること、電子透かし情報の検出のための回路規模が大きく、コスト負担が重いこと、電子透かし情報の検出のための処理時間が長くなるために、ドライブ本来の書き込み時間や読み出し時間の短縮化の妨げとなること等が存在する。

電子透かし情報を使用しないで、ＤＶＤ－Videoの違法なコピーを防止するために、ドライブが読み出しデータフィルタおよび書き込みデータフィルタを備えるものが提案されている。読み出しデータフィルタは、ディスクから読み出したデータがＤＶＤ－Videoデータのビデオ、オーディオ、サブピクチャの何れかの種類のパックであれば、当該パックに対してマスク処理を行い、それ以外の制御情報のパックであれば、マスク処理を行わずに、パックをバッファメモリへ転送する。マスク処理とは、対象のデータを無効データ例えば全てゼロのデータに置き換える処理を意味する。このようにしてＤＶＤ－Videoコンテンツの違法な再生を防止できる。

書き込みデータフィルタは、ＰＣから転送されてきたパックのパックヘッダを検出してパックの種類を判定し、データがＤＶＤ－Videoデータのビデオ、オーディオ、サブピクチャの何れかの種類のパックであれば、当該パックに対してマスク処理を行い、それ以外の制御情報のパックであれば、マスク処理を行わずに、パックをＤＶＤエンコーダへ転送する。したがって、ＰＣによってＤＶＤ－Videoのコンテンツが違法にコピーされることを防止することができる。

この方法は、ＰＣと書き込み可能なＤＶＤディスクとを利用した違法

な再生および記録をＤＶＤ－Videoのフォーマットに基づいて防止することができる。しかしながら、ＤＶＤ－Videoのフォーマットのデータの記録再生が一切できなくなる問題がある。この点を考慮して、ＰＣとドライブとの間で認証を行い、認証が成立しない時には、上述したようなＤＶＤドライブでコンテンツデータのマスク処理を行うモードとし、認証が成立した時には、コンテンツデータの暗号化／復号を行うモードとする方法が提案されている。この方法は、ＤＶＤ－Videoディスクを再生することを可能とする。しかしながら、先に提案されている方法では、書き込み時には、コンテンツデータに対してスクランブルをかけていない。

書き込みデータに対してスクランブルをかけていないために、既存のＤＶＤ－VideoのプレイヤーのＣＳＳを利用することができず、また、記録されたコンテンツデータが著作権が保護されたコンテンツとならない問題があった。たとえＣＳＳの暗号化を破る「ＤｅＣＳＳ」ソフトウェアが存在している状況下でも、記録されているコンテンツが正規のライセンス機関の承認を受けたＣＳＳでもってスクランブルがかけられていることは、著作権が保護されるコンテンツであることを明示する上で重要である。

よって、この発明の目的は、ドライブによって書き込み時に著作権保護技術例えばＣＳＳによって、書き込みデータを保護し、書き込まれたデータが保護の対象であることを明示することが可能な信号処理システム、記録再生装置、記録方法、記録方法のプログラム並びに記録媒体を提供することにある。

また、この発明は、著作権保護技術を一般ユーザの所有するＰＣのアプリケーションとして搭載する場合に、一般ユーザによる著作権保護技術の書き込みソフトウェアを作成させないようにできる信号処理システ

ム、記録再生装置、記録方法、記録方法のプログラム並びに記録媒体を提供することにある。

発明の開示

上述した課題を解決するために、この発明の第１の態様は、記録媒体から情報を読み出し、記録媒体に情報を記録する記録再生装置と、記録再生装置が伝達手段を介して接続される情報処理装置とを備え、管理機構が管理する第１の暗号化鍵と、記録媒体固有の第２の暗号化鍵と、記録の度に生成される第３の暗号化鍵とを使用したコンテンツ情報暗号化方法で暗号化されたコンテンツ情報を記録媒体に記録する信号処理システムであって、

記録再生装置は、

第１の暗号化鍵を保持する保持手段と、

記録媒体に暗号化されて記録されている第２の暗号化鍵を再生し、第１の暗号化鍵で復号する第２の暗号化鍵復号手段と、

第３の暗号化鍵を生成する第３の暗号化鍵生成手段と、

第３の暗号化鍵を復号された第２の暗号化鍵で暗号化する暗号化手段と、

情報処理装置との間の認証を行い、認証成立時にセッションキーを生成する認証手段と、

暗号化されて記録されている第２の暗号化鍵をセッションキーによってバス暗号化して情報処理装置に伝送する第１のバス暗号化手段と、

暗号化された第３の暗号化鍵をセッションキーによってバス暗号化して情報処理装置に伝送する第２のバス暗号化手段と、

情報処理装置からの暗号化およびバス暗号化されたコンテンツ情報をバス復号するバス復号手段と、

暗号化された第３の暗号化鍵と、暗号化されたコンテンツ情報を記録媒体に記録する記録手段とを有し、

情報処理装置は、

第１の暗号化鍵を保持する保持手段と、

記録再生装置との間の認証を行い、認証成立時にセッションキーを生成する認証手段と、

バス暗号化された第２の暗号化鍵をセッションキーによってバス復号して暗号化された第２の暗号化鍵を復号する第１のバス復号手段と、

暗号化された第２の暗号化鍵を第１の暗号化鍵で復号する復号手段と、

バス暗号化された第３の暗号化鍵をセッションキーによってバス復号して暗号化された第３の暗号化鍵を復号する第２のバス復号化手段と、

暗号化された第３の暗号化鍵を第２の暗号化鍵で復号する復号手段と、

記録再生装置に対して伝送するコンテンツ情報を第３の暗号化で暗号化する暗号化手段と、

暗号化されたコンテンツ情報をセッションキーでバス暗号化して記録再生装置に送出するバス暗号化手段とを有する信号処理システムである。

この発明の第２の態様は、記録媒体から情報を読み出し、記録媒体に情報を記録する記録再生装置と、記録再生装置が伝達手段を介して接続される情報処理装置とを備え、管理機構が管理する第１の暗号化鍵と、記録媒体固有の第２の暗号化鍵と、記録の度に生成される第３の暗号化鍵とを使用したコンテンツ情報暗号化方法で暗号化されたコンテンツ情報を記録媒体に記録する信号処理システムであって、

記録再生装置は、

第１の暗号化鍵を保持する保持手段と、

第２の暗号化鍵を生成する第２の暗号化鍵生成手段と、

生成された第２の暗号化鍵を第１の暗号化鍵で暗号化する暗号化手段

と、

第３の暗号化鍵を生成する第３の暗号化鍵生成手段と、

生成された第２の暗号化鍵で第３の暗号化鍵を暗号化する暗号化手段と、

情報処理装置との間の認証を行い、認証成立時にセッションキーを生成する認証手段と、

暗号化された第２の暗号化鍵をセッションキーによってバス暗号化して情報処理装置に伝送する第１のバス暗号化手段と、

暗号化された第３の暗号化鍵をセッションキーによってバス暗号化して情報処理装置に伝送する第２のバス暗号化手段と、

情報処理装置からの暗号化およびバス暗号化されたコンテンツ情報をバス復号するバス復号手段と、

暗号化された第２の暗号化鍵と、暗号化された第３の暗号化鍵と、暗号化されたコンテンツ情報を記録媒体に記録する記録手段とを有し、

情報処理装置は、

第１の暗号化鍵を保持する保持手段と、

記録再生装置との間の認証を行い、認証成立時にセッションキーを生成する認証手段と、

バス暗号化された第２の暗号化鍵をセッションキーによってバス復号して暗号化された第２の暗号化鍵を復号する第１のバス復号手段と、

暗号化された第２の暗号化鍵を第１の暗号化鍵で復号する復号手段と、

バス暗号化された第３の暗号化鍵をセッションキーによってバス復号して暗号化された第３の暗号化鍵を復号する第２のバス復号化手段と、

暗号化された第３の暗号化鍵を第２の暗号化鍵で復号する復号手段と、

記録再生装置に対して伝送するコンテンツ情報を第３の暗号化で暗号化する暗号化手段と、

暗号化されたコンテンツ情報をセッションキーでバス暗号化して記録再生装置に送出するバス暗号化手段とを有する信号処理システムである。

この発明の第３の態様は、記録媒体から情報を読み出し、記録媒体に情報を記録する記録再生装置と、記録再生装置が伝達手段を介して接続される情報処理装置とを備え、管理機構が管理する第１の暗号化鍵と、記録媒体固有の第２の暗号化鍵と、記録の度に生成される第３の暗号化鍵とを使用したコンテンツ情報暗号化方法で暗号化されたコンテンツ情報を記録媒体に記録する信号処理システムであって、

記録再生装置は、

第１の暗号化鍵を保持する保持手段と、

記録媒体に暗号化されて記録されている第２の暗号化鍵を再生し、第１の暗号化鍵で復号する第２の暗号化鍵復号手段と、

第３の暗号化鍵を生成する第３の暗号化鍵生成手段と、

第３の暗号化鍵を復号された第２の暗号化鍵で暗号化する暗号化手段と、

情報処理装置との間の認証を行い、認証成立時にセッションキーを生成する認証手段と、

情報処理装置からのバス暗号化されたコンテンツ情報をバス復号するバス復号手段と、

コンテンツ情報を第３の暗号化鍵によって暗号化する暗号化手段と、

暗号化された第３の暗号化鍵と、暗号化されたコンテンツ情報を記録媒体に記録する記録手段とを有し、

情報処理装置は、

記録再生装置との間の認証を行い、認証成立時にセッションキーを生成する認証手段と、

記録再生装置に対して伝送するコンテンツ情報をセッションキーでバ

ス暗号化して記録再生装置に送出するバス暗号化手段とを有する信号処理システムである。

この発明の第４の態様は、記録媒体から情報を読み出し、記録媒体に情報を記録する記録再生装置と、記録再生装置が伝達手段を介して接続される情報処理装置とを備え、管理機構が管理する第１の暗号化鍵と、記録媒体固有の第２の暗号化鍵と、記録の度に生成される第３の暗号化鍵とを使用したコンテンツ情報暗号化方法で暗号化されたコンテンツ情報を記録媒体に記録する信号処理システムであって、

記録再生装置は、

第１の暗号化鍵を保持する保持手段と、

第２の暗号化鍵を生成する第２の暗号化鍵生成手段と、

生成された第２の暗号化鍵を第１の暗号化鍵で暗号化する暗号化手段と、

第３の暗号化鍵を生成する第３の暗号化鍵生成手段と、

第３の暗号化鍵を生成された第２の暗号化鍵で暗号化する暗号化手段と、

情報処理装置との間の認証を行い、認証成立時にセッションキーを生成する認証手段と、

情報処理装置からのバス暗号化されたコンテンツ情報をバス復号するバス復号手段と、

コンテンツ情報を第３の暗号化鍵によって暗号化する暗号化手段と、

暗号化された第２の暗号化鍵と、暗号化された第３の暗号化鍵と、暗号化されたコンテンツ情報を記録媒体に記録する記録手段とを有し、

情報処理装置は、

記録再生装置との間の認証を行い、認証成立時にセッションキーを生成する認証手段と、

コンテンツ情報をセッションキーでバス暗号化して記録再生装置に送出するバス暗号化手段とを有する信号処理システムである。

この発明の第５の態様は、伝達手段を介して情報処理装置と接続され、記録媒体から情報を読み出し、記録媒体に情報を記録する記録再生装置であって、管理機構が管理する第１の暗号化鍵と、記録媒体固有の第２の暗号化鍵と、記録の度に生成される第３の暗号化鍵とを使用したコンテンツ情報暗号化方法で暗号化されたコンテンツ情報を記録媒体に記録する記録再生装置であって、

第１の暗号化鍵を保持する保持手段と、

記録媒体に暗号化されて記録されている第２の暗号化鍵を再生し、第１の暗号化鍵で復号する第２の暗号化鍵復号手段と、

第３の暗号化鍵を生成する第３の暗号化鍵生成手段と、

第３の暗号化鍵を復号された第２の暗号化鍵で暗号化する暗号化手段と、

情報処理装置との間の認証を行い、認証成立時にセッションキーを生成する認証手段と、

暗号化されて記録されている第２の暗号化鍵をセッションキーによってバス暗号化して情報処理装置に伝送する第１のバス暗号化手段と、

暗号化された第３の暗号化鍵をセッションキーによってバス暗号化して情報処理装置に伝送する第２のバス暗号化手段と、

情報処理装置からの暗号化およびバス暗号化されたコンテンツ情報をバス復号するバス復号手段と、

暗号化された第３の暗号化鍵と、暗号化されたコンテンツ情報を記録媒体に記録する記録手段とを有し、

暗号化およびバス暗号化されたコンテンツ情報は、第３の暗号化鍵で暗号化され、さらに、暗号化コンテンツ情報を情報処理装置で生成され

たセッションキーでバス暗号化したものである記録再生装置である。

この発明の第６の態様は、伝達手段を介して情報処理装置と接続され、記録媒体から情報を読み出し、記録媒体に情報を記録する記録再生装置であって、管理機構が管理する第１の暗号化鍵と、記録媒体固有の第２の暗号化鍵と、記録の度に生成される第３の暗号化鍵とを使用したコンテンツ情報暗号化方法で暗号化されたコンテンツ情報を記録媒体に記録する記録再生装置であって、

第１の暗号化鍵を保持する保持手段と、

第２の暗号化鍵を生成する第２の暗号化鍵生成手段と、

生成された第２の暗号化鍵を第１の暗号化鍵で暗号化する暗号化手段と、

第３の暗号化鍵を生成する第３の暗号化鍵生成手段と、

生成された第２の暗号化鍵で第３の暗号化鍵を暗号化する暗号化手段と、

情報処理装置との間の認証を行い、認証成立時にセッションキーを生成する認証手段と、

暗号化された第２の暗号化鍵をセッションキーによってバス暗号化して情報処理装置に伝送する第１のバス暗号化手段と、

暗号化された第３の暗号化鍵をセッションキーによってバス暗号化して情報処理装置に伝送する第２のバス暗号化手段と、

情報処理装置からの暗号化およびバス暗号化されたコンテンツ情報をバス復号するバス復号手段と、

暗号化された第２の暗号化鍵と、暗号化された第３の暗号化鍵と、暗号化されたコンテンツ情報を記録媒体に記録する記録手段とを有し、

暗号化およびバス暗号化されたコンテンツ情報は、第３の暗号化鍵で暗号化され、さらに、暗号化コンテンツ情報を情報処理装置で生成され

たセッションキーでバス暗号化したものである記録再生装置である。

この発明の第７の態様は、伝達手段を介して情報処理装置と接続され、記録媒体から情報を読み出し、記録媒体に情報を記録する記録再生装置であって、管理機構が管理する第１の暗号化鍵と、記録媒体固有の第２の暗号化鍵と、記録の度に生成される第３の暗号化鍵とを使用したコンテンツ情報暗号化方法で暗号化されたコンテンツ情報を記録媒体に記録する記録再生装置であって、

第１の暗号化鍵を保持する保持手段と、

記録媒体に暗号化されて記録されている第２の暗号化鍵を再生し、第１の暗号化鍵で復号する第２の暗号化鍵復号手段と、

第３の暗号化鍵を生成する第３の暗号化鍵生成手段と、

第３の暗号化鍵を復号された第２の暗号化鍵で暗号化する暗号化手段と、

情報処理装置との間の認証を行い、認証成立時にセッションキーを生成する認証手段と、

情報処理装置からのバス暗号化されたコンテンツ情報をバス復号するバス復号手段と、

コンテンツ情報を第３の暗号化鍵によって暗号化する暗号化手段と、

暗号化された第３の暗号化鍵と、暗号化されたコンテンツ情報を記録媒体に記録する記録手段とを有し、

バス暗号化されたコンテンツ情報は、暗号化コンテンツ情報を情報処理装置で生成されたセッションキーでバス暗号化したものである記録再生装置である。

この発明の第８の態様は、伝達手段を介して情報処理装置と接続され、記録媒体から情報を読み出し、記録媒体に情報を記録する記録再生装置であって、管理機構が管理する第１の暗号化鍵と、記録媒体固有の第２

の暗号化鍵と、記録の度に生成される第３の暗号化鍵とを使用したコンテンツ情報暗号化方法で暗号化されたコンテンツ情報を記録媒体に記録する記録再生装置であって、

第１の暗号化鍵を保持する保持手段と、

第２の暗号化鍵を生成する第２の暗号化鍵生成手段と、

生成された第２の暗号化鍵を第１の暗号化鍵で暗号化する暗号化手段と、

第３の暗号化鍵を生成する第３の暗号化鍵生成手段と、

第３の暗号化鍵を生成された第２の暗号化鍵で暗号化する暗号化手段と、

情報処理装置との間の認証を行い、認証成立時にセッションキーを生成する認証手段と、

情報処理装置からのバス暗号化されたコンテンツ情報をバス復号するバス復号手段と、

コンテンツ情報を第３の暗号化鍵によって暗号化する暗号化手段と、

暗号化された第２の暗号化鍵と、暗号化された第３の暗号化鍵と、暗号化されたコンテンツ情報を記録媒体に記録する記録手段とを有し、

バス暗号化されたコンテンツ情報は、暗号化コンテンツ情報を情報処理装置で生成されたセッションキーでバス暗号化したものである記録再生装置である。

この発明の第９の態様は、記録媒体から情報を読み出し、記録媒体に情報を記録する記録再生装置と、記録再生装置が伝達ステップを介して接続される情報処理装置とを備え、管理機構が管理する第１の暗号化鍵と、記録媒体固有の第２の暗号化鍵と、記録の度に生成される第３の暗号化鍵とを使用したコンテンツ情報暗号化方法で暗号化されたコンテンツ情報を記録媒体に記録する記録方法であって、

記録再生装置は、

第１の暗号化鍵を保持する保持ステップと、

記録媒体に暗号化されて記録されている第２の暗号化鍵を再生し、第１の暗号化鍵で復号する第２の暗号化鍵復号ステップと、

第３の暗号化鍵を生成する第３の暗号化鍵生成ステップと、

第３の暗号化鍵を復号された第２の暗号化鍵で暗号化する暗号化ステップと、

情報処理装置との間の認証を行い、認証成立時にセッションキーを生成する認証ステップと、

暗号化されて記録されている第２の暗号化鍵をセッションキーによってバス暗号化して情報処理装置に伝送する第１のバス暗号化ステップと、

暗号化された第３の暗号化鍵をセッションキーによってバス暗号化して情報処理装置に伝送する第２のバス暗号化ステップと、

情報処理装置からの暗号化およびバス暗号化されたコンテンツ情報をバス復号するバス復号ステップと、

暗号化された第３の暗号化鍵と、暗号化されたコンテンツ情報を記録媒体に記録する記録ステップとを実行し、

情報処理装置は、

第１の暗号化鍵を保持する保持ステップと、

記録再生装置との間の認証を行い、認証成立時にセッションキーを生成する認証ステップと、

バス暗号化された第２の暗号化鍵をセッションキーによってバス復号して暗号化された第２の暗号化鍵を復号する第１のバス復号ステップと、

暗号化された第２の暗号化鍵を第１の暗号化鍵で復号する復号ステップと、

バス暗号化された第３の暗号化鍵をセッションキーによってバス復号

して暗号化された第３の暗号化鍵を復号する第２のバス復号化ステップと、

暗号化された第３の暗号化鍵を第２の暗号化鍵で復号する復号ステップと、

記録再生装置に対して伝送するコンテンツ情報を第３の暗号化で暗号化する暗号化ステップと、

暗号化されたコンテンツ情報をセッションキーでバス暗号化して記録再生装置に送出するバス暗号化ステップとを実行する記録方法である。また、この発明は、記録方法のプログラムおよびプログラムが格納された記録媒体である。

この発明の第１０の態様は、記録媒体から情報を読み出し、記録媒体に情報を記録する記録再生装置と、記録再生装置が伝達ステップを介して接続される情報処理装置とを備え、管理機構が管理する第１の暗号化鍵と、記録媒体固有の第２の暗号化鍵と、記録の度に生成される第３の暗号化鍵とを使用したコンテンツ情報暗号化方法で暗号化されたコンテンツ情報を記録媒体に記録する記録方法であって、

記録再生装置は、

第１の暗号化鍵を保持する保持ステップと、

第２の暗号化鍵を生成する第２の暗号化鍵生成ステップと、

生成された第２の暗号化鍵を第１の暗号化鍵で暗号化する暗号化ステップと、

第３の暗号化鍵を生成する第３の暗号化鍵生成ステップと、

生成された第２の暗号化鍵で第３の暗号化鍵を暗号化する暗号化ステップと、

情報処理装置との間の認証を行い、認証成立時にセッションキーを生成する認証ステップと、

暗号化された第２の暗号化鍵をセッションキーによってバス暗号化して情報処理装置に伝送する第１のバス暗号化ステップと、

暗号化された第３の暗号化鍵をセッションキーによってバス暗号化して情報処理装置に伝送する第２のバス暗号化ステップと、

情報処理装置からの暗号化およびバス暗号化されたコンテンツ情報をバス復号するバス復号ステップと、

暗号化された第２の暗号化鍵と、暗号化された第３の暗号化鍵と、暗号化されたコンテンツ情報を記録媒体に記録する記録ステップとを実行し、

情報処理装置は、

第１の暗号化鍵を保持する保持ステップと、

記録再生装置との間の認証を行い、認証成立時にセッションキーを生成する認証ステップと、

バス暗号化された第２の暗号化鍵をセッションキーによってバス復号して暗号化された第２の暗号化鍵を復号する第１のバス復号ステップと、

暗号化された第２の暗号化鍵を第１の暗号化鍵で復号する復号ステップと、

バス暗号化された第３の暗号化鍵をセッションキーによってバス復号して暗号化された第３の暗号化鍵を復号する第２のバス復号化ステップと、

暗号化された第３の暗号化鍵を第２の暗号化鍵で復号する復号ステップと、

記録再生装置に対して伝送するコンテンツ情報を第３の暗号化で暗号化する暗号化ステップと、

暗号化されたコンテンツ情報をセッションキーでバス暗号化して記録再生装置に送出するバス暗号化ステップとを実行する記録方法である。

また、この発明は、記録方法のプログラムおよびプログラムが格納された記録媒体である。

この発明の第１１の態様は、記録媒体から情報を読み出し、記録媒体に情報を記録する記録再生装置と、記録再生装置が伝達ステップを介して接続される情報処理装置とを備え、管理機構が管理する第１の暗号化鍵と、記録媒体固有の第２の暗号化鍵と、記録の度に生成される第３の暗号化鍵とを使用したコンテンツ情報暗号化方法で暗号化されたコンテンツ情報を記録媒体に記録する記録方法であって、

記録再生装置は、

第１の暗号化鍵を保持する保持ステップと、

記録媒体に暗号化されて記録されている第２の暗号化鍵を再生し、第１の暗号化鍵で復号する第２の暗号化鍵復号ステップと、

第３の暗号化鍵を生成する第３の暗号化鍵生成ステップと、

第３の暗号化鍵を復号された第２の暗号化鍵で暗号化する暗号化ステップと、

情報処理装置との間の認証を行い、認証成立時にセッションキーを生成する認証ステップと、

情報処理装置からのバス暗号化されたコンテンツ情報をバス復号するバス復号ステップと、

コンテンツ情報を第３の暗号化鍵によって暗号化する暗号化ステップと、

暗号化された第３の暗号化鍵と、暗号化されたコンテンツ情報を記録媒体に記録する記録ステップとを実行し、

情報処理装置は、

記録再生装置との間の認証を行い、認証成立時にセッションキーを生成する認証ステップと、

記録再生装置に対して伝送するコンテンツ情報をセッションキーでバス暗号化して記録再生装置に送出するバス暗号化ステップとを実行する記録方法である。また、この発明は、記録方法のプログラムおよびプログラムが格納された記録媒体である。

この発明の第１２の態様は、記録媒体から情報を読み出し、記録媒体に情報を記録する記録再生装置と、記録再生装置が伝達ステップを介して接続される情報処理装置とを備え、管理機構が管理する第１の暗号化鍵と、記録媒体固有の第２の暗号化鍵と、記録の度に生成される第３の暗号化鍵とを使用したコンテンツ情報暗号化方法で暗号化されたコンテンツ情報を記録媒体に記録する記録方法であって、

記録再生装置は、

第１の暗号化鍵を保持する保持ステップと、

第２の暗号化鍵を生成する第２の暗号化鍵生成ステップと、

生成された第２の暗号化鍵を第１の暗号化鍵で暗号化する暗号化ステップと、

第３の暗号化鍵を生成する第３の暗号化鍵生成ステップと、

第３の暗号化鍵を生成された第２の暗号化鍵で暗号化する暗号化ステップと、

情報処理装置との間の認証を行い、認証成立時にセッションキーを生成する認証ステップと、

情報処理装置からのバス暗号化されたコンテンツ情報をバス復号するバス復号ステップと、

コンテンツ情報を第３の暗号化鍵によって暗号化する暗号化ステップと、

暗号化された第２の暗号化鍵と、暗号化された第３の暗号化鍵と、暗号化されたコンテンツ情報を記録媒体に記録する記録ステップとを実行

し、

情報処理装置は、

記録再生装置との間の認証を行い、認証成立時にセッションキーを生成する認証ステップと、

コンテンツ情報をセッションキーでバス暗号化して記録再生装置に送出するバス暗号化ステップとを実行する記録方法である。また、この発明は、記録方法のプログラムおよびプログラムが格納された記録媒体である。

この発明では、暗号化例えばＣＳＳ方式でコンテンツ情報を記録するので、記録されたコンテンツ情報は、著作権が保護されたものであることを明確とできる。すなわち、正規のライセンスを受けない違法な方法で、記録されているコンテンツ情報をコピーしたり、再生すれば、著作権を侵害していると主張することができる。この発明では、記録再生装置内で生成した暗号化鍵を記録再生装置自身がメディア例えばＤＶＤディスクへ書き込むことにより、ＣＳＳ方式でＤＶＤディスクへ記録をするときに、一般のＰＣユーザがＣＳＳ書き込みソフトウェアを作成できないようにできる。このことにより、正規に許可されたものだけがＣＳＳ書き込みアプリケーションを作成できるようになる。

この発明では、記録再生装置内で生成した暗号化鍵を記録再生装置自身がメディアへ書き込むことにより、ＣＰＲＭのように、鍵情報を予め記録ディスクへ記録済みとする必要がなくなることから、ディスク製造にかかるコストの低下に貢献する。

この発明では、ＰＣと記録再生装置の相互認証時の乱数データにメディアタイプを含めることによって、セキュアにメディアタイプを記録再生装置からＰＣへ伝えることが可能となる。このことから、ＰＣと記録再生装置間の標準化されたインターフェース上でのメディアタイプの改

ざんや、改造された記録再生装置による成りすまし行為を防止することができる。

この発明では、相互認証時の乱数データにコピー世代管理情報（ＣＧＭＳ）を含めることによって、セキュアにＣＧＭＳをＰＣから記録再生装置へ伝えることが可能となる。このことから、ＰＣと記録再生装置間の標準化されたインターフェース上でのＣＧＭＳの改ざんや、改造されたＰＣアプリケーションによる成りすまし行為を防止することができる。

この発明では、相互認証が成立しない間は、暗号化鍵のディスクへの書き込みを記録再生装置内のエンコーダＬＳＩ(Large Scale Integrated Circuit：大規模集積回路)で禁止し、その暗号化鍵書き込み禁止機能を相互認証の成立によって解除することにより、一般のユーザによるＣＳＳ書き込みソフトウェアの作成を禁止できる。このことにより、正規に許可されたものだけがＣＳＳ書き込みアプリケーションを作成できるようになる。

図面の簡単な説明

第１図は、ＣＳＳ方式でＲＯＭディスクへ記録する際の鍵情報の関係を示すブロック図である。

第２図は、ＣＳＳ方式で記録されたＲＯＭディスクを再生するＤＶＤプレーヤー内の鍵情報とスクランブルデータの再生の方法を示すブロック図である。

第３図は、ＲＯＭディスクのリードインエリアのデータ構成を示す略線図である。

第４図は、セクタの構成を示す略線図である。

第５図は、ＣＳＳ方式によるコピー防止機能を説明するための略線図である。

第６図は、ＣＳＳ方式で記録されたＲＯＭディスクを再生するＰＣとドライブでの鍵情報とスクランブルデータの再生の方法を示すブロック図である。

第７図は、第６図のシステムにおけるドライブとディスク間のデータの流れを示す略線図である。

第８図は、ディスクキーが書き込み済みの記録型ＤＶＤメディアへＣＳＳ方式でデータを書き込む際の記録方法の一例を示すブロック図である。

第９図は、ディスクキーが書き込み済みでない記録型ＤＶＤメディアへＣＳＳ方式でデータを書き込む際の記録方法の一例を示すブロック図である。

第１０図は、ディスクキーが書き込み済みの記録型ＤＶＤメディアへＣＳＳ方式でデータを書き込む際の記録方法をＰＣとドライブの組み合わせで実現する場合の一例を示すブロック図である。

第１１図は、第１０図の構成におけるドライブとディスク間のデータの流れを示す略線図である。

第１２図は、ディスクキーが書き込み済みでない記録型ＤＶＤメディアへＣＳＳ方式でデータを書き込む際の記録方法をＰＣとドライブの組み合わせで実現する場合の一例を示すブロック図である。

第１３図は、第１２図の構成におけるドライブとディスク間のデータの流れを示す略線図である。

第１４図は、第１０図の構成に対してスクランブルデータをバス暗号化して転送するようにした構成を示すブロック図である。

第１５図は、第１４図の構成におけるドライブとディスク間のデータの流れを示す略線図である。

第１６図は、第１２図の構成に対してスクランブルデータをバス暗号

化して転送するようにした構成を示すブロック図である。

第１７図は、第１６図の構成におけるドライブとディスク間のデータの流れを示す略線図である。

第１８図は、この発明の第１の実施形態の構成を示すブロック図である。

第１９図は、第１８図の構成におけるドライブとディスク間のデータの流れを示す略線図である。

第２０図は、この発明の第２の実施形態の構成を示すブロック図である。

第２１図は、第２０図の構成におけるドライブとディスク間のデータの流れを示す略線図である。

第２２図は、この発明の第３の実施形態の構成を示すブロック図である。

第２３図は、この発明の第４の実施形態の構成を示すブロック図である。

第２４図は、第１８図の構成に対してタイトルキーのマスク制御機構を加えたこの発明の第５の実施形態の構成を示すブロック図である。

第２５図は、第２０図の構成に対してディスクキーとタイトルキーのマスク制御機構を加えたこの発明の第６の実施形態の構成を示すブロック図である。

第２６図は、第２２図の構成に対してタイトルキーのマスク制御機構を加えたこの発明の第７の実施形態の構成を示すブロック図である。

第２７図は、第２３図の構成に対してディスクキーとタイトルキーのマスク制御機構を加えたこの発明の第８の実施形態の構成を示すブロック図である。

第２８図は、相互認証からセッションキーを生成する仕組みを示して

おり、同時にディスクタイプをセキュアにドライブからＰＣへ伝える仕組みを説明する略線図である。

第２９図は、ドライブ側におけるディスクタイプの情報の処理を説明するフローチャートである。

第３０図は、ＰＣ側におけるディスクタイプの情報の処理を説明するフローチャートである。

第３１図は、相互認証からセッションキーを生成する仕組みを示しており、同時にコピー世代管理情報をセキュアにドライブからＰＣへ伝える手段を説明する略線図である。

第３２図は、ＭＡＣ計算やセッションキー生成においてＡＥＳを利用した場合の例を示すブロック図である。

第３３図は、相互認証からセッションキー生成までのドライブ側の処理を示すフローチャートである。

第３４図は、相互認証からセッションキー生成までのＰＣ側の処理を示すフローチャートである。

第３５図は、バス暗号化／復号の処理の一例を示すブロック図である。

第３６図は、第３５図の処理の流れを示すフローチャートである。

第３７図は、ＡＶパックの構造とバス暗号化の対象範囲を説明するための略線図である。

第３８図は、１セクタのデータ構成を示す略線図である。

第３９図は、データの記録処理の流れを示す略線図である。

第４０図は、マスクコントロールが対象とするデータを説明するための略線図である。

第４１図は、マスクコントロールの構成の一例を示すブロック図である。

第４２図は、マスクコントロール内のフィルタの構成の一例（ＣＳＳ

キー書き込み禁止時）を示すブロック図である。

第４３図は、マスクコントロール内のフィルタの構成の一例（ＣＳＳキー書き込み禁止解除時）を示すブロック図である。

第４４図は、マスクコントロール内のフィルタの構成の応用例を示すブロック図である。

第４５図は、セッションキーの生成と消滅、およびＣＳＳキーのマスクコントロールの処理を示すフローチャートである。

第４６図は、マスターキーの生成方法の他の例を示すブロック図である。

発明を実施するための最良の形態

以下、この発明について説明するが、この発明の理解を容易とするために、ＤＶＤレコーダでＣＳＳ方式による記録を実現するために、考えられるいくつかの例とその場合の問題点について説明する。また、以下の説明では、ＤＶＤメディアへの記録についてのみ説明し、再生処理については、ＣＳＳ方式による再生処理と同様であるので、その説明を省略する。さらに、本明細書の特許請求の範囲において使用される用語と実施の形態中で使用される用語との対応関係について以下に説明する。

記録媒体：メディア例えばＤＶＤライタブルディスク、記録再生装置：ドライブ、情報処理装置：パーソナルコンピュータ、伝達手段：インターフェース、信号処理システム：メディアを記録再生するドライブとパーソナルコンピュータとがインターフェースを介して接続されるシステムである。

コンテンツ情報：メディアに記録すべき情報例えばオーディオ／ビジュアルデータをコンテンツ情報としている。第１の暗号化鍵：マスターキーである。第２の暗号化鍵：ディスクキーであり、ディスク上には、

キーである。第２の暗号化鍵：ディスクキーであり、ディスク上には、暗号化されたセキュアドディスクキーとして記録される。第３の暗号化鍵：タイトルキーであり、ディスク上には、暗号化され、暗号化タイトルキーとして記録される。

第８図は、ＤＶＤレコーダ５１ａにおいて、記録型ＤＶＤメディア（以下、ライタブルまたはレコーダブルディスクと適宜称する）１３ａへＣＳＳ方式でコンテンツを書き込む際の記録方法の一例を示す。ＤＶＤ－Videoと同様にライタブルディスク１３ａのリードインエリアの決められた場所に予めセキュアドディスクキー１０ａを書き込み済みとする例である。オーディオ／ビジュアルデータ６０がＤＶＤレコーダ５１ａのＭＰＥＧエンコーダ５２によって圧縮符号化され、スクランブラ５３によってスクランブルされ、スクランブルドＭＰＥＧデータ９がライタブルディスク１３ａに記録される。

ＤＶＤレコーダ５１ａの内部の乱数生成器（ＲＮＧ：Random Number Generator）５４によりタイトルキーが生成される。タイトルキーは、記録の度に生成され、また、ＣＧＭＳのステータスが変化した時にも生成される。スクランブラ５３は、タイトルキーを使用してＭＰＥＧデータをスクランブルする。タイトルキーは、エンクリプタ５５で暗号化され、ライタブルディスク１３ａに暗号化タイトルキー１１が記録される。記録済みのセキュアドディスクキー１０ａがデクリプタ５６において、マスターキー５７によって復号され、ディスクキーが得られる。

第９図に示す例は、ライタブルディスクに暗号化鍵情報であるセキュアドディスクキーを予め書き込み済みとしない例である。ＤＶＤレコーダ５１ｂが乱数発生器５４および５８を有し、乱数生成器５４および５８により、ディスクキーとタイトルキーを生成する。ディスクキーをＤＶＤレコーダ５１ｂがライタブルディスク１３ｂに書き込む。例えばブ

ランクディスクのフォーマッティングの処理によってディスクキーがライタブルディスク１３ｂに対して書かれる。後からディスクキーを書き込むことによって、ディスクキーを書き込み済みとする第８図の方法よりも記録型ＤＶＤメディアの製造コストを下げることが可能となる。

第１０図および第１２図にそれぞれ示す構成は、ＣＳＳ方式でスクランブルされたビデオコンテンツを記録型ＤＶＤメディアへ書き込む機能を、ＰＣとドライブの組み合わせで実現する場合の一例および他の例である。

これらの図において、参照符号６１がライタブルディスク１３ａまたは１３ｂに対してデータを記録し、また、再生する記録再生装置としてのＤＶＤドライブを示す。参照符号７１がデータ処理装置（ホスト）としてのＰＣを示し、ＰＣ７１に対してアプリケーションソフトウェアがインストールされ、ＤＶＤビデオエンコーダとしてＰＣ７１が機能する。但し、ソフトウェア処理に限定されるものではなく、ＤＶＤビデオエンコーダとしてハードウェア構成（基板構成）としても良い。

ＤＶＤドライブ６１とＰＣ７１との間がインターフェースで接続されている。インターフェースは、ＡＴＡＰＩ(AT Attachment with Packet Interface)，ＳＣＳＩ(Small Computer System Interface)，ＵＳＢ(Universal Serial Bus)，ＩＥＥＥ(Institute of Electrical and Electronics Engineers)１３９４等である。

ＤＶＤドライブ６１には、認証部６２、バスエンクリプタ６３およびバスデクリプタ６４が備えられている。ＰＣ７１には、認証部７２、バスデクリプタ７３およびバスエンクリプタ７４が備えられている。また、ＰＣ７１には、ＭＰＥＧエンコーダ５２、スクランブラ５３、乱数発生器５４、エンクリプタ５５、デクリプタ５６およびマスターキー５７が備えられている。オーディオ／ビジュアルデータ６０がＭＰＥＧエンコ

ーダ５２で、圧縮符号化され、ＤＶＤフォーマットの形式のストリームデータに変換される。スクランブラ５３にてタイトルキーによってスクランブルされてＤＶＤドライブ６１にインターフェースを介して供給され、ライタブルディスク１３ａ上にスクランブルドＭＰＥＧデータ９が記録される。

ＰＣ７１の内部の乱数生成器５４によりタイトルキーが生成される。スクランブラ５３は、タイトルキーを使用してＭＰＥＧデータをスクランブルする。タイトルキーは、エンクリプタ５５で暗号化され、認証が成立した時に生成されるセッションキーで暗号化タイトルキーがバスエンクリプタ７４で暗号化される。バスエンクリプタ７４の出力データがＤＶＤドライブ６１のバスデクリプタ６４に供給され、バスデクリプタ６４によってセッションキーで暗号化タイトルキーが復号される。ライタブルディスク１３ａに暗号化タイトルキー１１が記録される。

記録済みのセキュアドディスクキー１０ａがＤＶＤドライブ６１のバスエンクリプタ６３において、認証の成立によって生成されたセッションキーによって暗号化される。ＤＶＤドライブ６１からＰＣ７１へインターフェースを介して伝送され、バスデクリプタ７３においてセッションキーを使用して復号される。さらに、デクリプタ５６において、マスターキー５７によって復号され、ディスクキーが取得される。

第１１図は、第１０図に示すシステムにおいて、ＤＶＤドライブ６１とＰＣ７１との間の信号の授受の手順を示す。ＰＣ７１がＤＶＤドライブ６１に対してコマンドを送り、ＤＶＤドライブ６１がコマンドに応答した動作を行う。ライタブルディスクの挿入等でシーケンスが開始し、最初に認証シーケンスＡＫＥ（ステップＳ２１）がなされる。認証が成立すると、セッションキーＫｓをＤＶＤドライブ６１とＰＣ７１が共有する。認証が成立しなかった場合では、処理が中断する。

次に、ＰＣ７１からの要求に応じてＤＶＤドライブ６１がライタブルディスク１３ａ上のコントロールデータゾーンをシークし、コントロールデータを読み出す（ステップＳ２２）。次のステップＳ２３において、ＰＣ７１がセキュアドディスクキーを要求し、ＤＶＤドライブ６１がセキュアドディスクキーをリードする（ステップＳ２４およびＳ２５）。ＤＶＤドライブ６１がバスエンクリプタ６３によってセッションキーＫｓでセキュアドディスクキーを暗号化し、暗号化されたセキュアドディスクキーをＤＶＤドライブ６１がＰＣ７１に送る（ステップＳ２６）。ＰＣ７１のバスデクリプタ７３がセキュアドディスクキーを復号し、さらに、デクリプタ５６によってディスクキーを復号する。

次に、ステップＳ２７において、ＤＶＤドライブ６１が暗号化タイトルキーおよびＣＧＭＳをバスエンクリプタ７４において、セッションキーＫｓで暗号化し、ＤＶＤドライブ６１に対して送出する。さらに、ステップＳ２８において、スクランブラ５３からのスクランブルドＭＰＥＧデータがＤＶＤドライブ６１に送出される。ＤＶＤドライブ６１は、バスデクリプタ６においてセッションキーＫｓで復号した暗号化タイトルキーと、スクランブルドＭＰＥＧデータをライタブルディスク１３ａ上に記録する（ステップＳ２９）。

第１２図に示す構成例は、第１０図と比較すると、ライタブルディスク１３ｂに対してセキュアドディスクキーを記録する点で相違している。このため、乱数発生器５８がＰＣ７１に備えられ、ディスクキーが生成される。ディスクキーがエンクリプタ５９において、マスターキー５７によって暗号化され、セキュアドディスクキーがバスエンクリプタ７５において、セッションキーＫｓによって暗号化される。バスエンクリプタ７５の出力がＤＶＤドライブ６１にインターフェースを介して伝送され、バスデクリプタ６５において、セッションキーＫｓによって復号さ

れる。そして、ライタブルディスク１３ｂ上にセキュアドディスクキー１０ｂが記録される。他の構成は、第１０図に示すシステムと同様である。

第１３図は、第１２図に示すシステムにおけるＤＶＤドライブ６１とＰＣ７１との間の信号の授受の手順を示す。前述した第１０図のシステムにおける第１１図に示される手順と同様である。但し、バスエンクリプタ７５において、セッションキーＫｓで暗号化されたセキュアドディスクキーがＤＶＤドライブ６１に対して送出され（ステップＳ３３）、ＤＶＤドライブ６１がバスデクリプタ６５によってセッションキーＫｓで復号したセキュアドディスクキーをライタブルディスクに対してライトする処理（ステップＳ３４）が相違している。

上述した第１０図および第１２図に示す構成または方法を採用すると、一般ユーザが自作したＣＳＳ書き込みソフトウェアを使って作成したＣＳＳ暗号化データイメージを、通常のライトコマンドで書き込むことが可能という欠陥がある。理由は、ＣＳＳ方式のアルゴリズムは秘密とは言えず、公知とされていることによる。第１０図の例であれば、認証が成立した時点でアプリケーションソフトウェアを自作のものに切り替え、また、ライタブルディスク１３ａに予め記録されたセキュアドディスクキーに合わせて、自ら生成したタイトルキーを利用してコンテンツをスクランブルするＣＳＳスクランブラをＣＳＳ契約を受けない者が作成することが可能である。

次に、さらなる構成例について説明する。上述した第１０図および第１２図に示す構成または方法では、スクランブルドＭＰＥＧデータがＤＶＤドライブ６１とＰＣ７１間のＡＴＡＰＩ等の標準化されたインターフェースを通るために、書き込み中のスクランブルドＭＰＥＧデータが横から盗まれ、これに「ＤｅＣＳＳ」を施すことで平文に戻すという行

為がなされる危険性がある。この点を考慮してスクランブルドＭＰＥＧデータに対してもバス暗号化および復号を施すものが第１４図および第１６図にそれぞれ示す構成例である。

第１４図の構成例は、予めライタブルディスク１３ａ上にセキュアドディスクキー１０ａが記録されている点は、第１０図のシステムと同様である。第１０図のシステムと相違する点は、スクランブラ５３の出力に得られるスクランブルドＭＰＥＧデータがバスエンクリプタ７６によって暗号化されてからＤＶＤドライブ６１にインターフェースを介して伝送され、ＤＶＤドライブ６１において、バスデクリプタ６６によって復号されることである。これによって、インターフェースを通る時にスクランブルドＭＰＥＧデータが横取りされるおそれを少なくできる。

第１５図は、第１４図のシステムにおけるＤＶＤドライブ６１とＰＣ７１との間の信号の授受の手順を示す。この手順は、第１０図のシステムの手順を示す第１１図と同様のものである。相違する点は、ステップＳ２８において、スクランブルドＭＰＥＧデータを送る処理がステップＳ３８のセッションキーＫｓで暗号化されたスクランブルドＭＰＥＧデータを送ることに変わっていることである。

第１６図の構成例は、ライタブルディスク１３ｂ上にセキュアドディスクキー１０ｂを記録する点は、第１２図のシステムと同様である。第１２図のシステムと相違する点は、スクランブラ５３の出力に得られるスクランブルドＭＰＥＧデータがバスエンクリプタ７６によって暗号化されてからＤＶＤドライブ６１に伝送され、ＤＶＤドライブ６１において、バスデクリプタ６６によって復号されることである。これによって、インターフェースを通る時にスクランブルドＭＰＥＧデータが横取りされるおそれを少なくできる。例えば放送コンテンツから得られたスクランブルドＭＰＥＧデータを横取りしてハードディスクに記録し、その後

「ＤｅＣＳＳ」でもって復号することがされるおそれがある。

第１７図は、第１６図のシステムにおけるＤＶＤドライブ６１とＰＣ７１との間の信号の授受の手順を示す。この手順は、第１２図のシステムの手順を示す第１３図と同様のものである。相違する点は、ステップＳ２８において、スクランブルドＭＰＥＧデータを送る処理がステップＳ３８のセッションキーＫｓで暗号化されたスクランブルドＭＰＥＧデータを送ることに変わっていることである。

上述した第１４図および第１６図に示すさらなる構成または方法においても、一般ユーザが自作したＣＳＳ書き込みソフトウェアを使って作成したＣＳＳ暗号化データイメージを、通常のライトコマンドで書き込むことが可能という欠陥がある。

このように、ライタブルディスクに対する書き込みにＣＳＳを適用する場合に生じる問題を、この発明は、解決することができる。以下、図面を参照してこの発明のいくつかの実施形態について説明する。

第１８図は、この発明の第１の実施形態のシステム構成例を示す。参照符号１６１がＤＶＤドライブを示し、参照符号１７１がＤＶＤドライブ１６１と標準的なインターフェースで接続され、ホストとして機能する情報処理装置例えばＰＣである。ＰＣ１７１に対してアプリケーションソフトウェアがインストールされ、またはハードウェア（基板）が備えられることによって、ＰＣ１７１がＤＶＤビデオエンコーダとして機能する。例えばテレビジョンチューナの基板に対してハードウェアのビデオエンコーダ基板が組み込まれる構成とされる。第１の実施形態では、予めリードインエリアにセキュアドディスクキー１０ａが記録されているライタブルディスク１３ａが使用される。例えばライタブルディスクとしては、ＤＶＤ＋Ｒ／ＲＷ、またはＤＶＤ－Ｒ／ＲＷを使用できる。

ＤＶＤドライブ１６１は、タイトルキーを生成する乱数発生器８１と、

生成したタイトルキーをディスクキーで暗号化するエンクリプタ８２と、マスターキー８３と、セキュアドディスクキーをマスターキーで復号するデクリプタ８４とを内部に備えている。さらに、認証部６２、セッションキーＫｓでセキュアドディスクキーを暗号化するバスエンクリプタ６３、スクランブルドＭＰＥＧデータを復号するバスデクリプタ６６が備えられている。かかるＤＶＤドライブ１６１は、ＣＳＳ鍵発行センターの正規の承認を得てこれらの構成要素を備えたものである。また、ＤＶＤドライブ１６１は、ハードウェア（ＬＳＩ）で構成されているので、信号処理の内容を外部から知ることが不可能な耐タンパー性を有している。

ライタブルディスク１３ａから読まれたセキュアドディスクキー１０ａがデクリプタ８４においてマスターキー８３によって復号され、ディスクキーがエンクリプタ８２に供給される。エンクリプタ８２において、乱数発生器８１からのタイトルキーが暗号化され、暗号化タイトルキーが生成される。暗号化タイトルキーがＣＳＳ方式で規定されているようにライタブルディスク１３ａに対して記録される。

アプリケーションソフトウェアまたはハードウェア（基板）によってＤＶＤビデオエンコーダとしての機能をＰＣ１７１が有する。ＤＶＤドライブ１６１の認証部６２およびＰＣ１７１の認証部７２の相互認証が成立すると、セッションキーＫｓが生成される。ＤＶＤドライブ１６１のバスエンクリプタ６３において、セッションキーＫｓによってセキュアドディスクキーが暗号化され、バスエンクリプタ８５において、セッションキーＫｓによって暗号化タイトルキーが暗号化される。これらの暗号化されたデータが標準的インターフェースを介してＰＣ１７１に伝送される。

ＰＣ１７１では、バスデクリプタ７３において、セッションキーＫｓ

によってセキュアドディスクキーが復号され、バスデクリプタ７７において、セッションキーＫｓによって暗号化タイトルキーが復号される。デクリプタ５６において、マスターキー５７によってディスクキーが復号され、デクリプタ７８において、バスデクリプタ７７からの暗号化タイトルキーがディスクキーによって復号され、タイトルキーが得られる。

オーディオ／ビジュアルデータ６０がＭＰＥＧエンコーダ５２において、ＭＰＥＧ２によって圧縮符号化されると共に、ＤＶＤ規格のフォーマットのデータへ変換される。例えばＭＰＥＧエンコーダ５２では、ディジタル放送等で受信されたトランスポートストリームがプログラムストリームへ変換され、ＤＶＤフォーマットのデータへ変換される。ＭＰＥＧエンコーダ５２の出力データがスクランブラ５３にてタイトルキーによってスクランブルされる。スクランブラ５３からのスクランブルドＭＰＥＧデータがバスエンクリプタ７６において、セッションキーＫｓによって暗号化される。バスエンクリプタ７６の出力データがインターフェースを介してＤＶＤドライブ１６１に伝送される。ＤＶＤドライブ１６１では、バスデクリプタ６６によってスクランブルドＭＰＥＧデータが復号され、スクランブルドＭＰＥＧデータがライタブルディスク１３ａに記録される。なお、ＰＣ１７１において、ＭＰＥＧエンコーダ５２以外の構成要素は、ＣＳＳ鍵発行センターの正規の承認を得て備えたものである。

第１９図は、第１８図に示すシステムにおいて、ＤＶＤドライブ１６１とＰＣ１７１との間の信号の授受の手順を示す。ＰＣ１７１がＤＶＤドライブ１６１に対してコマンドを送り、ＤＶＤドライブ１６１がコマンドに応答した動作を行う。ライタブルディスクの挿入等でシーケンスが開始し、最初に認証シーケンスＡＫＥ（ステップＳ４１）がなされる。認証が成立すると、セッションキーＫｓをＤＶＤドライブ１６１とＰＣ

１７１が共有する。認証が成立しなかった場合では、処理が中断する。

次に、ＰＣ１７１からの要求に応じてＤＶＤドライブ１６１がライタブルディスク１３ａ上のコントロールデータゾーンをシークし、コントロールデータを読み出す（ステップＳ４２）。次のステップＳ４３において、ＰＣ１７１がセキュアドディスクキーを要求し、ＤＶＤドライブ１６１がセキュアドディスクキーをリードする（ステップＳ４４およびＳ４５）。ＤＶＤドライブ１６１がバスエンクリプタ６３によってセッションキーＫｓでセキュアドディスクキーを暗号化し、暗号化されたセキュアドディスクキーをＤＶＤドライブ１６１がＰＣ１７１に送る（ステップＳ４６）。ＰＣ１７１のバスデクリプタ７３がセッションキーＫｓによってセキュアドディスクキーを復号し、さらに、デクリプタ５６によってディスクキーを復号する。

次に、ステップＳ４７において、認証シーケンスＡＫＥがなされる。認証が成立すると、セッションキーＫｓが新たに生成され、このセッションキーＫｓをＤＶＤドライブ１６１とＰＣ１７１が共有する。認証が成立しなかった場合では、処理が中断する。認証が成立すると、ステップＳ４８において、ＰＣ１７１がＣＧＭＳをＤＶＤドライブ１６１に対して送る。ステップＳ４９において、ＰＣ１７１がＤＶＤドライブ１６１に対してセッションキーＫｓで暗号化されたタイトルキーを要求する。

ＤＶＤドライブ１６１は、エンクリプタ８２からの暗号化タイトルキーをエンクリプタ８５に供給し、セッションキーＫｓで暗号化タイトルキーを暗号化する。このエンクリプタ８５からのＫｓで暗号化された暗号化タイトルキーをＰＣ１７１に対して戻す（ステップＳ５０）。

ＰＣ１７１では、バスデクリプタ７７および７８による復号処理によってタイトルキーを生成し、スクランブラ５３において、ＭＰＥＧデータを暗号化し、スクランブルドＭＰＥＧデータを生成する。さらに、ス

クランブルドＭＰＥＧデータをバスエンクリプタ７６においてセッションキーＫｓで暗号化し、Ｋｓで暗号化されたスクランブルドＭＰＥＧデータをＤＶＤドライブ１６１に伝送する（ステップＳ５１）。ＤＶＤドライブ１６１は、バスデクリプタ６６においてセッションキーＫｓで受け取ったデータを復号してスクランブルドＭＰＥＧデータを得る。そして、スクランブルドＭＰＥＧデータと暗号化タイトルキーをライタブルディスク１３ａ上にライトする（ステップＳ５２）。

上述した第１の実施形態は、ドライブ１６１内で生成したタイトルキーをセキュアにＰＣ１７１へ転送してＰＣ側でのＣＳＳスクランブルに利用し、ＰＣ１７１から受け取ったＣＳＳスクランブルＭＰＥＧデータとドライブ１６１で生成したタイトルキーをライタブルディスク１３ａへ書き込む方法である。したがって、第１の実施形態は、ＰＣ側でタイトルキーを改ざんさせないと同時に、勝手に作成されたタイトルキーでＣＳＳスクランブルをさせないことができ、ライセンスを受けないものが自由にＣＳＳスクランブル書き込みソフトウェアを作ることを防止することができる。

第２０図は、この発明の第２の実施形態のシステム構成を示す。第２の実施形態は、ライタブルディスク１３ｂに対してセキュアドディスクキーを記録するものである。ＤＶＤドライブ１６１は、タイトルキー生成用の乱数発生器８１に加えて、ディスクキー生成用の乱数発生器８６が設けられている。ディスクキーがタイトルキーをエンクリプタ８２において暗号化するために使用される。また、ディスクキーがマスターキー８３によってエンクリプタ８７で暗号化され、セキュアドディスクキーが生成される。セキュアドディスクキー１０ｂがライタブルディスク１３ｂ上のリードインエリアに記録される。

このように、ディスクキーを生成し、生成したディスクキーを暗号化

してセキュアドディスクキーを生成し、セキュアドディスクキー１０ｂをリードインエリアに記録することを除くと、第２の実施形態の構成および処理は、第１８図に示す第１の実施形態のものと同様である。

第２１図は、第２０図に示すシステムにおいて、ＤＶＤドライブ１６１とＰＣ１７１との間の信号の授受の手順を示す。第２１図に示されるものは、第１９図に示す信号の授受の手順と同様である。相違する点は、セキュアドディスクキーをＰＣ１７１が要求した時に、ＤＶＤドライブ１６１がセキュアドディスクキーをライタブルディスク１３ｂに記録するステップＳ５４と、このセキュアドディスクキーをセッションキーＫｓで暗号化してＰＣ１７１に戻す点である。

第２の実施形態は、ドライブ１６１内で生成したディスクキーとタイトルキーをセキュアにＰＣ１７１へ転送してＰＣ側ビデオエンコーダーでのＣＳＳスクランブルに利用し、ＰＣ１７１から受け取ったスクランブルドＭＰＥＧデータと、ドライブ１６１で生成したセキュアドディスクキーと、暗号化タイトルキーをライタブルディスクへ書き込む方法である。かかる第２の実施形態は、ＰＣ側でタイトルキーを改ざんさせないと同時に、勝手に作成されたタイトルキーでＣＳＳスクランブルをさせないことから、ライセンスを受けないものが自由にＣＳＳスクランブル書き込みソフトウェアを作ることを防止する効果がある。さらに、ＤＶＤメディアへ予めディスクキーを記録しておく必要がないことから、メディアの製造コストを低くすることができる。

第２２図を参照して第３の実施形態について説明する。第３の実施形態では、ライタブルディスク１３ａのリードインエリアに予めセキュアドディスクキーが記録されている。セキュアドディスクキー１０ａは、マスターキー８３によってデクリプタ８４において復号され、ディスクキーが得られる。タイトルキーは、ＤＶＤドライブ２６１内の乱数発生

号化される。エンクリプタ８２からの暗号化タイトルキー１１がライタブルディスク１３ａ上に記録される。

ＤＶＤドライブ２６１は、認証部９１を有し、ＰＣ２７１の認証部９２と相互認証を行う。認証が成立するとセッションキーＫｓをＤＶＤドライブ２６１とＰＣ２７１とが共有する。この相互認証の方法は、ＣＳＳ方式と同様のものに限らず、後述するような新たな方法を採用できる。新たな認証方法を採用することによって、ライセンスを受けないものによるＣＳＳ書き込みソフト作成をより確実に防ぐことが可能となる。

ＰＣ２７１は、認証部９２を有する以外には、オーディオ／ビジュアルデータ６０を符号化するＭＰＥＧエンコーダ５２とバスエンクリプタ９３とを有するのみである。その他の処理は、ＤＶＤドライブ２６１においてなされる。ＰＣ２７１は、ＣＳＳスクランブルするための一切の鍵や処理を持たず、相互認証機能を持つのみであり、負荷が著しく軽くなる。

ＤＶＤドライブ２６１は、ＰＣ２７１からのセッションキーＫｓで暗号化されたＭＰＥＧデータをバスデクリプタ９４においてセッションキーＫｓで復号する。そして、スクランブラ９５で暗号化し、スクランブルドＭＰＥＧデータ９をライタブルディスク１３ａ上に記録する。スクランブラ９５は、乱数発生器８１によって生成されたタイトルキーによってＭＰＥＧデータを暗号化し、スクランブルドＭＰＥＧデータを生成する。

第３の実施形態も、ＰＣ側でタイトルキーを改ざんさせないと同時に、勝手に作成されたタイトルキーでＣＳＳスクランブルをさせないことから、ライセンスを受けないものが自由にＣＳＳスクランブル書き込みソフトウェアを作ることを防止する効果がある。新たな認証方法を導入すれば、ライセンスを受けない者によって書き込みソフトウェアが作成さ

フトウェアを作ることを防止する効果がある。新たな認証方法を導入すれば、ライセンスを受けない者によって書き込みソフトウェアが作成されることをより確実に防止できる。さらに、ＰＣ側の負荷を軽くすることができる。

第２３図は、第４の実施形態を示す。第３の実施形態と相違する点は、ＤＶＤドライブ２６１の乱数発生器８６によってディスクキーを生成し、ディスクキーをエンクリプタ８７においてマスターキー８３によって暗号化し、セキュアドディスクキー１０ｂをライタブルディスク１３ｂに対して記録することである。第３の実施形態と同様に、ＰＣ２７１が認証部９２と、バスエンクリプタ９３と、ＭＰＥＧエンコーダ５２を有する。

かかる第４の実施形態も上述した第３の実施形態と同様の作用効果を奏するものである。さらに、ＤＶＤメディアへ予めディスクキーを記録しておく必要がないことから、メディアの製造コストを低くすることができる。

第２４図は、第１８図に示す第１の実施形態の構成に対して暗号化タイトルキーのマスク制御機構としてのマスクコントロール１０１を加えた第５の実施形態を示す。マスクコントロール１０１に対してエンクリプタ８２からの暗号化タイトルキーが入力され、マスクコントロール１０１の出力に取り出された暗号化タイトルキー１１がライタブルディスク１３ａ上に記録される。

マスクコントロール１０１は、ＤＶＤドライブ１６１の認証部６２の認証の結果に応答してマスク機能が制御される。すなわち、ＰＣ１７１とＤＶＤドライブ１６１の相互認証が成立し、セッションキーＫｓが生成されている間はマスク機能が解除され、暗号化タイトルキー１１がライタブルディスク１３ａ上に記録される。一方、認証が成立しなければ

マスク機能は有効となり、暗号化タイトルキー１１が無効データまたはダミーデータ例えばゼロデータに置き換えられ、暗号化タイトルキーのライタブルディスク１３ａ上への書き込みが実質的に禁止される。

第２５図は、第２０図に示す第２の実施形態の構成に対して暗号化タイトルキーのマスク制御機構としてのマスクコントロール１０１と、セキュアドディスクキーのマスク制御機構としてのマスクコントロール１０２とを加えた第６の実施形態を示す。マスクコントロール１０１と同様に、マスクコントロール１０２は、セキュアドディスクキーに対してマスク機能を発揮する。すなわち、ＰＣ１７１とＤＶＤドライブ１６１の相互認証が成立し、セッションキーＫｓが生成されている間はマスク機能が解除され、セキュアドディスクキー１０ｂがライタブルディスク１３ｂ上に記録される。一方、認証が成立しなければマスク機能は有効となり、セキュアドディスクキー１０ｂがライタブルディスク１３ｂ上に記録されない。

上述した第５および第６の実施形態のように、ディスクへのＣＳＳキーの書き込みを相互認証の成立結果によって制御することによって、一般のユーザによるＣＳＳ書き込みソフトウェアの作成をより確実に禁止することが可能となる。それによって正規に許可された者だけがＣＳＳ書き込みアプリケーションソフトウェアを作成することができる。

第２６図は、第２２図に示す第３の実施形態の構成に対して暗号化タイトルキーのマスク制御機構としてのマスクコントロール１０３を加えた第７の実施形態を示す。マスクコントロール１０３に対してエンクリプタ８２からの暗号化タイトルキーが入力され、マスクコントロール１０３の出力に取り出された暗号化タイトルキー１１がライタブルディスク１３ａ上に記録される。

マスクコントロール１０３は、ＤＶＤドライブ１６１の認証部６２の

認証の結果に応答してマスク機能が制御される。すなわち、ＰＣ１７１とＤＶＤドライブ１６１の相互認証が成立し、セッションキーＫｓが生成されている間はマスク機能が解除され、暗号化タイトルキー１１がライタブルディスク１３ａ上に記録される。一方、認証が成立しなければマスク機能は有効となり、暗号化タイトルキー１１がライタブルディスク１３ａ上に記録されない。

第２７図は、第２３図に示す第４の実施形態の構成に対して暗号化タイトルキーのマスク制御機構としてのマスクコントロール１０３と、セキュアドディスクキーのマスク制御機構としてのマスクコントロール１０４とを加えた第８の実施形態を示す。マスクコントロール１０３と同様に、マスクコントロール１０４は、セキュアドディスクキーに対してマスク機能を発揮する。すなわち、ＰＣ１７１とＤＶＤドライブ１６１の相互認証が成立し、セッションキーＫｓが生成されている間はマスク機能が解除され、セキュアドディスクキー１０ｂがライタブルディスク１３ｂ上に記録される。一方、認証が成立しなければマスク機能は有効となり、セキュアドディスクキー１０ｂがライタブルディスク１３ｂ上に記録されない。

上述した第７および第８の実施形態のように、ディスクへのＣＳＳキーの書き込みを相互認証の成立結果によって制御することによって、一般のユーザによるＣＳＳ書き込みソフトウェアの作成をより確実に禁止することが可能となる。それによって正規に許可された者だけがＣＳＳ書き込みアプリケーションソフトウェアを作成することができる。

第２８図は、上述した第３の実施形態（第２２図）、第４の実施形態（第２３図）、第７の実施形態（第２６図）および第８の実施形態（第２７図）のそれぞれに備えられている認証部９１および９２に適用される認証構成または方法の一例を説明するものである。第２８図に示す例

では、相互認証からセッションキーを生成すると同時に、ディスクタイプの情報をセキュアにドライブからＰＣへ伝えるようにしている。ディスクタイプデータは、下記のように定義された２ビットの情報である。

（０，０）：ＲＯＭ　（０，１）：未定義　（１，０）：ライタブル　タイプ１　（１，１）：ライタブルディスク　タイプ２

例えばタイプ１は、リライタブルディスクを示し、タイプ２は、１回のみ記録可能なディスクを示す。他の例としては、タイプ１がＣＳＳ方式の書き込みが許されている種類のディスクを意味し、タイプ２がＣＳＳ方式の書き込みが許されていない種類のディスクを意味する。ディスクタイプは、ディスク上のリードインエリア内の所定位置に記録されている。但し、ウォブリンググルーブの情報に記録されているものであっても良く、また、ディスクの光学的特性から判定されたものでも良い。第２８図において、参照符号３０１がディスクタイプデータを示す。

ディスクタイプデータ３０１がマルチプレクサ３０２および３０３にそれぞれ供給され、乱数発生器３０４および３０５からの乱数と混合され、ディスクタイプデータを含む６４ビットの乱数データRa1およびRa2がそれぞれ生成される。例えば６４ビットの乱数中の所定の２ビットのビット位置例えば下位側の２ビットにディスクタイプデータが配置される。この乱数Ra1およびRa2がＰＣ側に伝送され、デマルチプレクサ４０１によって乱数Ra1からディスクタイプデータ３０１をＰＣが得ることができる。ＰＣは、取得したディスクタイプのデータに対応するアプリケーションソフトウェアを実行する。

ＤＶＤドライブ１６１の認証部９１は、認証キーＫｍを有する。認証キーＫｍは、多くの場合にＬＳＩ内部に配置され、外部から読み出すことができないようセキュアに記憶される。ドライブ１６１がＣＳＳによる記録を扱う正当なドライブとなるためには、認証キーＫｍのような著

作権保護技術に関する秘密情報を必要とするので、正規のライセンスを受けずに正規品になりすますようなクローン・ドライブの作成が防止される。

参照符号３０６、３０７および３０８は、認証キーＫｍをパラメータとしてＭＡＣ値を計算するＭＡＣ(Message Authentication Code)演算ブロックをそれぞれ示す。また、参照符号３０４、３０５および３０９が６４ビットの乱数を発生する乱数発生器である。上述したように、ディスクタイプと乱数とがマルチプレクサ３０２で合成されてマルチプレクサ３０２から乱数Ｒa1が出力され、この乱数Ｒa1がＭＡＣ演算ブロック３０６に供給される。マルチプレクサ３０３からの乱数Ｒa2がＭＡＣ演算ブロック３０７に供給される。さらに、乱数発生器３０９が乱数Ｒa3を生成する。乱数発生器３０４、３０５、３０９は、例えばＬＳＩの構成の乱数発生器であり、ソフトウェアにより乱数を発生する方法と比較してより真正乱数に近い乱数を発生することができる。乱数発生器を共通のハードウエアとしても良いが、乱数Ｒa1、Ｒa2、Ｒa3は、互いに独立したものである。

ＰＣ側の認証部９２も、認証キーＫｍを有し、認証キーＫｍをパラメータとしてＭＡＣ値を計算するＭＡＣ演算ブロック４０６、４０７および４０８を備えている。さらに、それぞれ６４ビットの乱数Ｒb1，Ｒb2，Ｒb3をそれぞれ発生する乱数発生器４０４、４０５および４０９が備えられている。乱数２８Ｒb1，Ｒb2，Ｒb3は、ＰＣ側の認証部９２のＭＡＣ演算ブロック４０６、４０７および４０８にそれぞれ供給されると共に、ＤＶＤドライブ側に伝送され、ＭＡＣ演算ブロック３０６、３０７、３０８に対して供給される。乱数発生器４０４、４０５、４０９は、通常はソフトウェアによって乱数を発生するものであるが、ハードウェアによる乱数が利用できる場合にはこれを用いても良い。

ＤＶＤドライブの認証部９１において生成された乱数と、ＰＣの認証部９２において生成された乱数とが交換される。すなわち、乱数Ｒa1および乱数Ｒb1がＭＡＣ演算ブロック３０６および４０６に入力され、乱数Ｒa2および乱数Ｒb2がＭＡＣ演算ブロック３０７および４０７に入力され、乱数Ｒa3および乱数Ｒb3がＭＡＣ演算ブロック３０８および４０８に入力される。

ＭＡＣ演算ブロック３０６が演算したＭＡＣ値と、ＭＡＣ演算ブロック４０６が演算したＭＡＣ値とが認証部９２内の比較４１０において比較され、二つの値が同一か否かが判定される。ここでのＭＡＣ値は、eKm(Ra1 ‖ Rb1)と表記される。ｅＫｍ（）は、認証キーＫｍを鍵として括弧内のデータを暗号化することを表している。Ｒa1 ‖ Ｒb1の記号は、左側に乱数Ｒa1を配し、右側に乱数Ｒb1を配するように、二つの乱数を結合することを表している。比較の結果、二つの値が同一と判定されると、ＰＣによるＤＶＤドライブの認証が成功したことになり、そうでない場合には、この認証が失敗したことになる。

ＭＡＣ演算ブロック３０７が演算したＭＡＣ値と、ＭＡＣ演算ブロック４０７が演算したＭＡＣ値とがドライブの認証部９１内の比較３１０において比較され、二つの値が同一か否かが判定される。ここでのＭＡＣ値は、eKm(Rb2 ‖ Ra2)と表記される。比較の結果、二つの値が同一と判定されると、ＤＶＤドライブによるＰＣの認証が成功したことになり、そうでない場合には、この認証が失敗したことになる。

かかる相互認証において、比較３１０および４１０の両者において、ＭＡＣ値が同一と判定され、ＤＶＤドライブおよびＰＣの両者の正当性が確認されると、すなわち、相互認証が成功すると、ＭＡＣ演算ブロック３０８および４０８によって、共通のセッションキーeKm(Ra3 ‖ Rb3)がそれぞれ生成される。このように、互いのＭＡＣ計算値を交換して一

の認証のみを行うようにしても良い。

ディスクタイプデータの他の例を下記に示す。

（０，０）：ＲＯＭ　（０，１）：未定義（通常の書き込み可能）

（１，０）：未定義（通常の書き込み可能）　（１，１）：ビデオライタブルディスク（ＣＳＳ／ＣＰＲＭによるビデオ記録が可能で、私的録画補償金がディスク販売価格に含まれているディスク）

このように定義されたディスクタイプデータが上述したようにＰＣ側に伝送される乱数に混合した場合に、ドライブ側の処理およびＰＣ側の処理の一例を説明する。第２９図は、ドライブ側の処理を示すフローチャートである。

冒頭に挙げた非特許文献３に記載されているように、ディスク上には、ウォブリングしたグルーブが予め形成されている。ウォブリングは、ＡＤＩＰ(Address in Pre-groove)と称される情報によって変調されたものである。ＡＤＩＰに含まれる情報の一つがメディアタイプ（３バイト）である。最初のステップＳＴ１０１において、メディアタイプが判別される。判別結果がＲＯＭか否かがステップＳＴ１０２において判定される。ＲＯＭであれば、ステップＳＴ１０３において、ディスクタイプがＲＯＭ（０，０）と判定される。ＲＯＭでない場合には、ステップＳＴ１０４において、ディスクアプリケーションコードがビデオライタブルか否かが判定される。

ＡＤＩＰに含まれる情報の他のものがディスクアプリケーションコード（１バイト）である。ディスクアプリケーションコードは、特別のアプリケーションにのみ使用されるように制限されたディスクであるか否かを識別するのに使用される。例えばディスクアプリケーションコードによって、ビデオ信号を書き込むことが可能なこと（ビデオライタブル）が識別される。

によって、ビデオ信号を書き込むことが可能なこと（ビデオライタブル）が識別される。

ステップＳＴ１０４において、ディスクアプリケーションコードがビデオライタブルであれば、ディスクタイプがビデオライタブルと判定される（ステップＳＴ１０６）。若し、ステップＳＴ１０４において、ディスクアプリケーションコードがビデオライタブルでないと判定されると、ディスクタイプがリザーブド（すなわち、未定義）と判定される（ステップＳＴ１０５）。

このようにドライブが判定したディスクタイプが上述したように、相互認証時に交換される乱数に混合されたＰＣ側へ伝送される。第３０図は、ＰＣ側の処理を示すフローチャートである。ステップＳＴ１１１において、相互認証がなされ、ステップＳＴ１１２において、ＰＣがドライブからディスクタイプデータを取得する。

ディスクタイプがＲＯＭがどうかがステップＳＴ１１３において判定される。ＲＯＭと判定されると、ステップＳＴ１１４において、データの書き込みが禁止される。ＲＯＭでないと判定されると、ステップＳＴ１１５において、ディスクタイプがビデオライタブルか否かが判定される。ビデオライタブルでないと判定されると、ステップＳＴ１１６において、データ書き込みが可能と判定される。ビデオライタブルであると判定されると、ステップＳＴ１１７において、ＣＳＳ／ＣＰＲＭによる書き込み可能と判定される。

第３１図は、認証部９１および９２の他の例を示す。他の例は、上述した一例が相互認証に加えて、ディスクタイプの情報をＤＶＤドライブからＰＣへ伝える機能を有するのに対して、ＣＧＭＳの情報をＰＣからＤＶＤに伝えるものである。

ＰＣ９の認証部９２には、記録しようとするＣＧＭＳデータ４１１が

存在する。ＣＧＭＳデータ４１１は、記録すべきビデオデータに含まれる著作権管理情報に基づいた２ビットのデータであり、以下のように定義された２ビットの情報である。

（０，０）：コピーフリー　（０，１）：ＥＰＮ(Encryption Plus Non-assertion)（ディジタル放送におけるコンテンツ管理情報）　（１，０）：１回のコピーのみ許可　（１，１）：コピー禁止

ＣＧＭＳデータ４１１は、記録しようとするビデオ入力から分離されたものである。例えば分離されたＣＧＭＳデータが（１，０）で１回のコピーのみ許可されている場合では、ライタブルディスクに記録されるＣＧＭＳデータは、１回コピーがされた結果、（１，１）のコピー禁止に変更される。

ＰＣ側の認証部９２において、ＣＧＭＳデータ４１１がマルチプレクサ４１２および４１３にそれぞれ供給され、乱数発生器４０４および４０５からの乱数と混合され、ＣＧＭＳデータを含む６４ビットの乱数データＲb1およびＲb2がそれぞれ生成される。例えば６４ビットの乱数中の所定の２ビットのビット位置例えば下位側の２ビットにＣＧＭＳデータが配置される。この乱数Ｒb1およびＲb2がＤＶＤドライブ側に伝送され、デマルチプレクサ３１１によって乱数Ｒb2からＣＧＭＳデータ４１１をＤＶＤドライブが得ることができる。ＣＧＭＳデータ４１１がライタブルディスク上の所定の位置に記録される。

第３２図は、ＭＡＣ演算ブロック３０６，３０７，３０８，４０６，４０７，４０８として、ＡＥＳ(Advanced Encryption Standard)エンクリプタを使用した場合の構成例を示す。二つの乱数ＡおよびＢを結合した１２８ビットの乱数Ａ‖Ｂと認証キーＫｍとがＡＥＳエンコーダに供給され、認証キーＫｍを鍵として乱数Ａ‖Ｂを暗号化した出力eKm(A‖B)が形成される。

さらに、第２８図に示す構成の場合における相互認証の処理の流れを第３３図および第３４図のフローチャートを参照して説明する。第３３図のフローチャートは、ＤＶＤドライブ側の認証部９１の処理の流れを示し、第３４図は、ＰＣ側の認証部９２の処理の流れを示す。最初に、第３４図中のステップＳＴ２１において、コマンドSEND KEYにより、認証部９１に対して乱数発生器４０４および４０５でそれぞれ生成された乱数Ｒb1と乱数Ｒb2が転送される。第３３図中のステップＳＴ１１において、認証部９１が認証部９２から転送されたこれらの乱数を受け取る。

その後、認証部９２は、コマンドREPORT KEYにより認証部９１に対して認証キーＫｍを鍵としたＭＡＣによるレスポンス値と乱数Ra1（ディスクタイプデータを含む）とを認証部９２へ転送することを要求する（ステップＳＴ２２）。このレスポンス値は、eKm(Ra1 ‖ Rb1)と表記される。ｅＫｍ（）は、認証キーＫｍを暗号鍵として括弧内のデータを暗号化することを表している。Ｒa1 ‖ Ｒb1の記号は、左側に乱数Ｒa1を配し、右側に乱数Ｒb1を配するように、二つの乱数を結合することを表している。

認証部９２からコマンドREPORT KEYを受け取った認証部９１は、ステップＳＴ１２において、ＭＡＣ演算ブロック３０６が生成したＭＡＣ値eKm(Ra1 ‖ Rb1)と乱数Ｒa1を認証部９２へ転送する。ステップＳＴ２３において、認証部９２は、自身のＭＡＣ演算ブロック４０６でＭＡＣ値を計算し、比較４１０において認証部９１から受け取った値と一致するかの確認を行う。若し、受け取ったＭＡＣ値と計算されたＭＡＣ値とが一致すれば、認証部９２（ＰＣ）による認証部９１（ＤＶＤドライブ）の認証が成功したことになる。ステップＳＴ２３における比較の結果が同一でない場合には、認証部９２（ＰＣ）による認証部９１（ＤＶ

Ｄドライブ）の認証が失敗したことになり、リジェクト処理がなされる。

認証部９２による認証部９１の認証が成功した場合には、ステップＳＴ２４において、認証部９２が認証部９１へコマンドREPORT KEYを送付し、認証部９１から乱数Ｒa2（ディスクタイプデータを含む）と乱数Ｒa3の転送を要求する。このコマンドに応答して、ステップＳＴ１３において、認証部９１は、これらの乱数を認証部９２へ転送する。

ステップＳＴ２５において、認証部９２のＭＡＣ演算ブロック４０７は、認証部９１から受け取った乱数から認証部９２が持つ認証キーＫｍを鍵としたＭＡＣによるレスポンス値eKm(Rb2‖Ra2)を計算し、乱数Ｒｂ3とともに、コマンドSEND KEYを用いて認証部９１へ転送する。

ステップＳＴ１４において、認証部９１は、認証部９２からレスポンス値eKm(Rb2‖Ra2)および乱数Rb3を受け取ると、自身でＭＡＣ値を計算し、ステップＳＴ１５において、比較３１０によって認証部９２から受け取ったＭＡＣ値と一致するかの確認を行う。若し、受け取ったＭＡＣ値と計算されたＭＡＣ値とが一致すれば、認証部９１（ＤＶＤドライブ）による認証部９２（ＰＣ）の認証が成功したことになる。この場合には、ステップＳＴ１６において、ＭＡＣ演算ブロック３０８がセッションキーeKm(Ra3‖Rb3)を生成し、また、認証部９２に対して認証が成功したことを示す情報を送信し、認証処理が完了する。セッションキーは、認証動作の度に異なる値となる。

ステップＳＴ１５における比較の結果が同一でない場合には、認証部９１による認証部９２の認証が失敗したことになり、ステップＳＴ１７において、認証が失敗したことを示すエラー情報が認証部９２に送信される。

認証部９２は、送付したコマンドSEND KEYに対する応答として認証部９１から認証が成功したか否かを示す情報を受け取り、受け取った情

報に基づいてステップＳＴ２６において、認証完了か否かを判断する。認証が成功したことを示す情報を受け取ることで認証完了と判断し、認証が失敗したことを示す情報を受け取ることで認証が完了しなかったと判断する。認証が完了した場合は、ステップＳＴ２７において、ＭＡＣ演算ブロック４０８がドライブ側と共通のセッションキーeKm(Ra3‖Rb3)（例えば６４ビット長）を生成する。認証が完了しなかった場合には、リジェクト処理がなされる。

上述したこの発明の全ての実施形態においては、ＰＣからＤＶＤドライブへ伝送される記録データをバスエンクリプタで暗号化し、ＤＶＤドライブでは、バスデクリプタで復号している。第３５図において、参照符号５０１がバスエンクリプタを示し、参照符号５１１がバスエンクリプタを示す。

ＰＣからＤＶＤドライブに対しては、２ＫＢ（キロバイト）のセクタデータからなるパックでもってデータが伝送される。パックは、パックヘッダによってパックの種類が指定されている。ＡＶパック検出部５０２は、オーディオパック、ビデパックおよびサブピクチャパックを検出し、検出結果に応じて制御信号を出力する。

ＡＶパック検出部５０２からの制御信号によってセレクタ５０３が制御される。入力データがオーディオパック、ビデパックおよびサブピクチャパックの場合には、入力データをＡＶデータエンクリプタ５０４に導き、セッションキーによって暗号化する。但し、パックヘッダは、暗号化されない。また、これらのパック以外の場合では、入力データを暗号化しないで、インターフェースを介してＤＶＤドライブに伝送する。

バスデクリプタ５１１のＡＶパック検出部５１２において、受け取ったパックの種類をパックヘッダから検出する。セレクタ５１３がＡＶパック検出部５１２からの制御信号で制御される。パックがオーディオパ

ック、ビデパックおよびサブピクチャパックの場合には、受取データをＡＶデータデクリプタ５１４に導き、セッションキーによって復号する。

ＣＳＳ方式で保護の対象となるのは、オーディオ／ビジュアルデータであるので、コンピュータのファイルデータ等の他の一般的データを暗号化する必要がない。そのために、ＡＶパックのみを暗号化している。

第３６図は、バス暗号化／復号の処理の流れを示す。ステップＳＴ３１において、パックヘッダ検出部の検出結果からビデオパックか否かが判定される。ビデオパックであれば、ステップＳＴ３２において、データが暗号化／復号される。ビデオパックでなければ、ステップＳＴ３３のオーディオパックか否かの判定ステップに処理が移る。

ステップＳＴ３３において、オーディオパックと判定されれば、ステップＳＴ３２においてデータが暗号化／復号され、そうでないと判定されれば、ステップＳＴ３４のサブピクチャパックか否かの判定ステップに処理が移る。ステップＳＴ３４において、サブピクチャパックと判定されれば、ステップＳＴ３２においてデータが暗号化／復号され、そうでないと判定されれば、データを暗号化／復号しない（ステップＳＴ３５）。そして、バス暗号化／復号の処理が終了する。

第３７図は、ＤＶＤビデオデータのオーディオパック、ビデオパックまたはサブピクチャパックの構成を示す。パックの制御情報が配置されたパックヘッダが先頭に配置され、その後にパケットヘッダが配置され、その後にオーディオデータ（ＡＣ３データ）、ビデオデータ（ＭＰＥＧプログラムストリーム）またはサブピクチャデータ（字幕等のテキストデータ）が配置される。パックヘッダおよびパケットヘッダは、可変長データであるので、これらのデータ長が最も長い場合を考慮して、パックヘッダおよびパケットヘッダを含む例えば１２８バイトがバス暗号化／復号の対象外とされ、残りの１９２０バイトがバス暗号化／復号の対

象とされる。合計の２Ｋ（２０４８）バイトが１セクタのメインデータとされる。

上述した第５の実施形態（第２４図）、第６の実施形態（第２５図）、第７の実施形態（第２６図）および第８の実施形態（第２７図）では、ＤＶＤドライブとＰＣとの相互認証が成立したか否かに応じて制御されるマスクコントロール１０１、１０２、、１０３、１０４を設けている。これらのマスクコントロールのマスクの対象とするデータについて説明する。最初にライタブルディスクに記録されるデータの構成について説明する。

ＤＶＤドライブでは、ＰＣから受け取ったデータをセクタ構造に変換してライタブルディスクに記録する。第３８図は、１セクタのデータ構成を示す。２Ｋバイトのメインデータに対して１２バイトのセクタヘッダが付加され、また、最後の４バイトがセクタ全体の対するエラー検出コードＥＤＣとされ、全体で２０６４バイトのデータセクタが構成されている。

セクタヘッダの先頭の４バイトがセクタ番号等のＩＤであり、その後の２バイトがＩＤに対するエラー検出用コードＩＥＤであり、その後の６バイトがコピー管理用データＣＰＲ＿ＭＡＩ(Copyright Management Information)である。ＣＰＲ＿ＭＡＩは、コピー管理（著作権管理）が必要なデータがメインデータとして記録される場合に必要なデータである。ＣＰＲ＿ＭＡＩ内にメインデータを復号するのに必要な暗号化タイトルキーが配置されている。

第３８図に示すセクタ構造のデータを記録時に生成する処理を第３９図を参照して説明する。第３９図に示すように、セクタヘッダのＩＤが用意される。このＩＤは、ＤＶＤドライブ内のＣＰＵによって生成される。すなわち、記録時にＰＣからライトコマンドがＤＶＤドライブに対

して伝送され、書き込みコマンドにディスクへの記録位置を示すＬＢＡ(Logical Block Address)データと、ライトデータ長のデータが付加されている。ＤＶＤドライブのＣＰＵは、ライトコマンドの指示内容が実行可能であると判断すると、ライトデータ長の分だけ、ＰＣからドライブのバッファメモリに対して２Ｋバイトのパック単位でデータを伝送させて蓄える。

そして、実際にライト動作を開始する前に、ＬＢＡデータからディスク上の物理的アドレスであるＰＳＮ(Physical Sector Number)を計算し、その値をＩＤとする。そのＩＤに対してエラー検出コードＩＥＤが付加され、ＩＤ＋ＩＥＤ（６バイト）が形成される。

さらに、（ＩＤ＋ＩＥＤ）データに対してＣＰＲ＿ＭＡＩおよびメインデータが付加され、さらに、これらのデータからセクタ毎のエラー検出符号ＥＤＣが生成され（ステップＳＴ４１）、スクランブルされる前の１単位（１フレーム）のデータが形成され、その１単位のデータ内のメインデータに対してタイトルキーでスクランブルが施され、スクランブルドメインデータを含むフレームが形成される（ステップＳＴ４２）。

さらに、スクランブルが施されたフレームを１６フレーム集めたデータに対してエラー訂正符号化を行う（ステップＳＴ４３）。エラー訂正符号化で生成されたＥＣＣが付加された１６フレームのデータ内のメインデータに対してインターリーブ処理が施される（ステップＳＴ４４）。そして、セクタ毎に２６シンクフレームを変調する（ステップＳＴ４５）。変調処理後のデータがライタブルディスクに記録される。

第４０図は、６バイトのＣＰＲ＿ＭＡＩのより詳細なデータ構成を示す。第４０図Ａは、（ＰＳＮ＜０３０００００ｈ）のリードインエリア内のＣＰＲ＿ＭＡＩのデータ構成を示し、第４０図Ｂは、（ＰＳＮ≧０３０００００ｈ）のデータエリア内のＣＰＲ＿ＭＡＩのデータ構成を示す。

第４０図Ａに示すリードインエリア内のＣＰＲ＿ＭＡＩは、一種の属性情報であり、書かれているデータがセキュアドディスクキーであることを示す情報が含まれている。先頭の１バイトＢＰ０が著作権保護システムタイプを示す。例えば著作権保護システムタイプがＣＳＳ対応か否か、並びにＣＰＲＭ対応のものか否かが示される。

次のバイトＢＰ１は、セキュアドディスクキーモードである。次のバイトＢＰ２およびＢＰ３は、未定義である。次のバイトＢＰ４の上位の２ビットが未定義とされ、下位の６ビットがビデオ認証コントロールコードとされる。さらに、バイトＢＰ５が地域（リージョン）管理情報とされている。

第４０図Ａにおいて破線で囲んで示すように、リードインエリア内のＣＰＲ＿ＭＡＩの全てのデータがマスクの対象とされる。すなわち、認証が成立しないでマスクを行う時には、リードインエリア内のＣＰＲ＿ＭＡＩの全てのデータが例えば００ｈのデータに書き換えられる。ビデオ認証コントロールコードは必ずしもマスクしないでも良い。なお、後述するマスクコントロールのためのＣＰＲ＿ＭＡＩフィルタにおいては、リードインエリア内のＣＰＲ＿ＭＡＩの中で、所定の暗号化方式（例えばＣＳＳ方式）であることを示す情報は、先頭のバイトＢＰ０であるので、このバイトＢＰ０を暗号化方式を示す情報以外の情報例えば００ｈのデータに書き換えることで、実質的にＣＰＲ＿ＭＡＩの全てのデータのマスクを行うようにしている。

第４０図Ｂに示すデータエリア内のＣＰＲ＿ＭＡＩについて説明すると、先頭のバイトＢＰ０にＣＰＭ（１ビット）、ＣＰ＿ＳＥＣ（１ビット）、ＣＧＭＳ（２ビット）、ＣＰＳ＿ＭＯＤ（４ビット）が配置されている。そして、残りの５バイトＢＰ１～ＢＰ５に対して暗号化ビデオタイトルキーが上位側から下位側に向かって順に配置されている。

第４０図Ｂにおいて破線で囲んで示すように、データエリア内のＣＰＲ＿ＭＡＩの内の先頭バイトＢＰ０以外のバイトＢＰ１－ＢＰ５（暗号化ビデオタイトルキー）がマスクの対象とされる。すなわち、認証が成立しないでマスクを行う時には、リードインエリア内のＣＰＲ＿ＭＡＩのバイトＢＰ１－ＢＰ５が例えば００ｈのデータに書き換えられる。

第４１図は、リードインエリア内並びにデータエリア内のＣＰＲ＿ＭＡＩに対するマスクコントロールの構成の一例を示す。この例では、第３９図に示される記録処理において、ＥＤＣを加えるステップＳＴ４１の直前でマスクコントロールを行うようにしている。第４１図において、参照符号６０１がセクタ情報（１バイト）が蓄えられているレジスタであり、参照符号６０２がＰＳＮ（３バイト）が蓄えられているレジスタである。これらの４バイトのＩＤが演算部６０３に入力され、２バイトのエラー検出符号ＩＥＤが算出される。

参照符号６０４は、ＣＰＲ＿ＭＡＩ（６バイト）が蓄えられているレジスタである。参照符号６０５は、１セクタのメインデータ（２Ｋバイト）が蓄えられているバッファメモリである。ＣＰＲ＿ＭＡＩがＣＰＲ＿ＭＡＩフィルタ６０６に入力され、マスクコントロールの処理を受ける。フィルタ６０６の出力にマスクコントロールされたＣＰＲ＿ＭＡＩ、すなわち、ＲＳＶ（６バイト）が取り出される。

エラー検出符号ＩＥＤ（２バイト）と、ＲＳＶ（６バイト）と、セクタ情報（１バイト）と、ＰＳＮ（３バイト）と、メインデータ（２０４８バイト）とが演算部６０７に入力され、演算部６０７によってセクタ全体のエラー検出符号ＥＤＣが生成される。参照符号６０８で示すミキサーに対してセクタ情報、ＰＳＮ、エラー検出コードＩＥＤ、ＲＳＶ、メインデータ、ＥＤＣが入力され、第３８図に示す構成の１セクタのデータが構成される。

互認証前の段階で、ＣＳＳキーの書き込みを禁止するためのマスクを行う場合の構成を示す。なお、第４２図、後述する第４３図および第４４図において、破線が囲んだＣＰＲ＿ＭＡＩフィルタ６０６は、論理ゲートによって構成されている。ディスク上のアドレスであるＰＳＮ（３バイト）が比較器６１１に入力され、所定のアドレス例えば０３００００ｈと比較される。また、ＣＰＲ＿ＭＡＩおよび乱数発生器６１３の生成した乱数がデータ変換器６１２に供給される。データ変換器６１２は、比較器６１１によって制御される。

データ変換器６１２は、リードインエリアとデータエリアとを指示する比較器６１１の出力によって、各エリアに応じた処理を行う。比較器６１１の出力によって、（ＰＳＮ＜０３００００ｈ）と判定される場合は、リードインエリアに記録されるＣＰＲ＿ＭＡＩ（第４０図Ａ参照）に対するマスクが行われる。マスクを行うために、データ変換器６１２がＢＰ０を００ｈのデータへ置き換える。比較器６１１の出力が（ＰＳＮ＜０３００００ｈ）以外を示す場合では、データエリアに記録されるＣＰＲ＿ＭＡＩ（第４０図Ｂ参照）に対するマスクが行われる。すなわち、ＢＰ０以外の５バイトが全て００ｈのデータに置き換えられる。

第４３図は、相互認証が成立してＣＳＳ方式の書き込みが許可される場合、すなわち、ＣＳＳキーの書き込み禁止の解除時のＣＰＲ＿ＭＡＩフィルタ６０６の処理を示す。

比較器６１１の出力によって、（ＰＳＮ＜０３００００ｈ）と判定されるリードインエリアでは、ＣＰＲ＿ＭＡＩ（第４０図Ａ参照）が出力される。また、（ＰＳＮ＜０３００００ｈ）以外の場合では、ＣＰＲ＿ＭＡＩ（第４０図Ｂ参照）が出力される。タイトルキーを生成するために、６バイト長の乱数発生器６１３が使用され、乱数発生器６１３が発生した６バイトの内の５バイトがＣＰＲ＿ＭＡＩの５バイト（ＢＰ１，

に、６バイト長の乱数発生器６１３が使用され、乱数発生器６１３が発生した６バイトの内の５バイトがＣＰＲ＿ＭＡＩの５バイト（ＢＰ１，ＢＰ２、ＢＰ３，ＢＰ４、ＢＰ５）として用いられる。

第４４図は、マスクコントロールの応用例を示す。応用例は、相互認証の成立をトリガーとしてリードインエリアのＢＰ１～ＢＰ５を乱数で埋めることを許可する例であり、ディスクキーのマスクコントロールに対して適用することができる。

比較器６１１の出力によってリードインエリアであることが決定される場合では、ＢＰ０が００ｈとされ、ＢＰ１～ＢＰ５が乱数発生器６１４の出力によって生成された乱数データとされる。このＢＰ０～ＢＰ５の６バイトがディスクのリードインエリアに記録されるので、そのディスクに固有のユニークＩＤが記録される。一方、データエリアでは、タイトルキーを記録する場合と異なり、ＢＰ０以外のＢＰ１～ＢＰ５の５バイトが全て００ｈとされる。

第４５図は、セッションキーの生成および消滅と、ＣＳＳキー（暗号化タイトルキーおよびセキュアドディスクキー、または暗号化タイトルキー）のマスク制御の処理の流れを示すフローチャートである。最初のステップＳＴ５１では、この発明の対象とするＣＳＳスクランブル書き込みが許可されたディスク例えばＤＶＤ＋ＲＷ／＋Ｒディスクが挿入されたか否かが判定される。ディスクが挿入されたと判定されると、ステップＳＴ５２においてＰＣアプリケーションが起動されているか否かが判定される。すなわち、ＰＣが電源オン、あるいは再起動を経て、ＯＳが起動しＰＣからアプリケーションプログラムの実行が可能か否かが判定される。ＣＳＳキー書き込みマスク機能は、デフォルトで書き込みを禁止する状態にある。なお、ステップＳＴ５１およびＳＴ５２の順序は、逆であっても良い。

ＰＣアプリケーションが起動されていると、ステップＳＴ５２で判定されると、ステップＳＴ５３において、相互認証がなされ、セッションキーが生成される。セッションキーの生成が完了したか否かがステップＳＴ５４において判定され、若し、完了したと判定されると、ＣＳＳキーの書き込みマスク機能が解除される（ステップＳＴ５５）。

ステップＳＴ５６において、ＰＣアプリケーションが終了したか否かが判定される。ＰＣアプリケーションが終了したと判定されると、ステップＳＴ５７において、ＰＣ内で生成されたセッションキーが消去される（ステップＳＴ５７）。そして、ＰＣアプリケーションが再び起動されているかどうかが判定される（ステップＳＴ５８）。起動されていると判定されると、ステップＳＴ５３に制御が戻る。

ステップＳＴ５８において、アプリケーションが起動されていないと判定されると、ＤＶＤ＋ＲＷ／＋Ｒディスクが排出されたか否かがステップＳＴ５９において判定される。排出されていないと判定されると、制御がステップＳＴ５８に戻る。ディスクが排出されたとステップＳＴ５９において判定されると、ステップＳＴ６０において、ドライブ内で生成したセッションキーが消去される。そして、マスクコントロールによってＣＳＳキー書き込みが禁止される（ステップＳＴ６１）。

ステップＳＴ５６において、アプリケーションが起動されていないと判定されると、ＤＶＤ＋ＲＷ／＋Ｒディスクが排出されたか否かがステップＳＴ６２において判定される。排出されていないと判定されると、制御がステップＳＴ５６に戻る。ディスクが排出されたとステップＳＴ６２において判定されると、ステップＳＴ６３において、ドライブ内で生成したセッションキーが消去される。そして、マスクコントロールによってＣＳＳキー書き込みが禁止される（ステップＳＴ６１）。

なお、マスターキーの配信構成を特開２００２－２３６６２２号公報

に記載されているようなツリー構造を使用しても良い。第４６図は、第２６図に示す実施の形態に対してこの方法を適用した場合の構成を示す。ドライブ２６１には、複数のドライブで共通のデバイスノードキー１１１およびドライブ固有のデバイスＩＤ１１２を保持する。また、ライタブルディスク１３ａには、ＥＫＢ(Enable Key Block)１４と呼ばれるブロックデータによって構成されるテーブルが格納されている。ＥＫＢには、複数の暗号化キーが含まれる。

ライタブルディスクからＥＫＢが復号部１１３に読み込まれ、復号部１１３において、デバイスノードキー１１１と、デバイスＩＤ１１２とによってマスターキーが復号される。この方法は、新たなマスターキーの配布、或いはマスターキーの更新に利用することができる。

この発明は、上述したこの発明の一実施形態等に限定されるものでは無く、この発明の要旨を逸脱しない範囲内で様々な変形や応用が可能である。例えばマスターキー、ディスクキーおよびタイトルキーの３つの暗号化鍵を使用する暗号化方法であれば、ＣＳＳ方式以外の暗号化方法を使用しても良い。また、この発明は、ディスク以外に光カード、メモリカード等の媒体に対して情報を記録する場合に対しても適用することができる。

請　求　の　範　囲

1．記録媒体から情報を読み出し、記録媒体に情報を記録する記録再生装置と、上記記録再生装置が伝達手段を介して接続される情報処理装置とを備え、管理機構が管理する第１の暗号化鍵と、記録媒体固有の第２の暗号化鍵と、記録の度に生成される第３の暗号化鍵とを使用したコンテンツ情報暗号化方法で暗号化されたコンテンツ情報を記録媒体に記録する信号処理システムであって、

上記記録再生装置は、

第１の暗号化鍵を保持する保持手段と、

記録媒体に暗号化されて記録されている第２の暗号化鍵を再生し、上記第１の暗号化鍵で復号する第２の暗号化鍵復号手段と、

第３の暗号化鍵を生成する第３の暗号化鍵生成手段と、

上記第３の暗号化鍵を復号された第２の暗号化鍵で暗号化する暗号化手段と、

情報処理装置との間の認証を行い、認証成立時にセッションキーを生成する認証手段と、

上記暗号化されて記録されている第２の暗号化鍵を上記セッションキーによってバス暗号化して上記情報処理装置に伝送する第１のバス暗号化手段と、

暗号化された上記第３の暗号化鍵を上記セッションキーによってバス暗号化して上記情報処理装置に伝送する第２のバス暗号化手段と、

上記情報処理装置からの暗号化およびバス暗号化されたコンテンツ情報をバス復号するバス復号手段と、

上記暗号化された上記第３の暗号化鍵と、上記暗号化されたコンテンツ情報を記録媒体に記録する記録手段とを有し、

上記情報処理装置は、

第１の暗号化鍵を保持する保持手段と、

上記記録再生装置との間の認証を行い、認証成立時にセッションキーを生成する認証手段と、

上記バス暗号化された第２の暗号化鍵を上記セッションキーによってバス復号して暗号化された上記第２の暗号化鍵を復号する第１のバス復号手段と、

上記暗号化された第２の暗号化鍵を上記第１の暗号化鍵で復号する復号手段と、

上記バス暗号化された第３の暗号化鍵を上記セッションキーによってバス復号して上記暗号化された第３の暗号化鍵を復号する第２のバス復号化手段と、

上記暗号化された第３の暗号化鍵を上記第２の暗号化鍵で復号する復号手段と、

上記記録再生装置に対して伝送するコンテンツ情報を上記第３の暗号化で暗号化する暗号化手段と、

上記暗号化されたコンテンツ情報を上記セッションキーでバス暗号化して上記記録再生装置に送出するバス暗号化手段とを有する信号処理システム。

２．請求の範囲１において、

上記記録再生装置の上記認証手段と上記情報処理装置の上記認証手段とは、生成した乱数データを交換する時に、上記記録再生装置から上記情報処理装置に伝送する乱数に上記記録媒体の種類の情報を混合するようにした信号処理システム。

３．請求の範囲１において、

上記記録再生装置の上記認証手段と上記情報処理装置の上記認証手段とは、生成した乱数データを交換する時に、上記情報処理装置から上記

記録再生装置に伝送する乱数に著作権関連情報を混合するようにした信号処理システム。

４．請求の範囲１において、

さらに、暗号化された上記第３の暗号化鍵に対するマスク制御手段を有し、

上記認証手段によって認証が成立している期間のみ、暗号化された上記第３の暗号化鍵の上記記録媒体に対する書き込みが可能とされた信号処理システム。

５．記録媒体から情報を読み出し、記録媒体に情報を記録する記録再生装置と、上記記録再生装置が伝達手段を介して接続される情報処理装置とを備え、管理機構が管理する第１の暗号化鍵と、記録媒体固有の第２の暗号化鍵と、記録の度に生成される第３の暗号化鍵とを使用したコンテンツ情報暗号化方法で暗号化されたコンテンツ情報を記録媒体に記録する信号処理システムであって、

上記記録再生装置は、

第１の暗号化鍵を保持する保持手段と、

第２の暗号化鍵を生成する第２の暗号化鍵生成手段と、

生成された第２の暗号化鍵を第１の暗号化鍵で暗号化する暗号化手段と、

第３の暗号化鍵を生成する第３の暗号化鍵生成手段と、

生成された第２の暗号化鍵で上記第３の暗号化鍵を暗号化する暗号化手段と、

情報処理装置との間の認証を行い、認証成立時にセッションキーを生成する認証手段と、

上記暗号化された第２の暗号化鍵を上記セッションキーによってバス暗号化して上記情報処理装置に伝送する第１のバス暗号化手段と、

暗号化された上記第３の暗号化鍵を上記セッションキーによってバス暗号化して上記情報処理装置に伝送する第２のバス暗号化手段と、

上記情報処理装置からの暗号化およびバス暗号化されたコンテンツ情報をバス復号するバス復号手段と、

上記暗号化された上記第２の暗号化鍵と、上記暗号化された上記第３の暗号化鍵と、上記暗号化されたコンテンツ情報を記録媒体に記録する記録手段とを有し、

上記情報処理装置は、

第１の暗号化鍵を保持する保持手段と、

上記記録再生装置との間の認証を行い、認証成立時にセッションキーを生成する認証手段と、

上記バス暗号化された第２の暗号化鍵を上記セッションキーによってバス復号して暗号化された上記第２の暗号化鍵を復号する第１のバス復号手段と、

上記暗号化された第２の暗号化鍵を上記第１の暗号化鍵で復号する復号手段と、

上記バス暗号化された第３の暗号化鍵を上記セッションキーによってバス復号して上記暗号化された第３の暗号化鍵を復号する第２のバス復号化手段と、

上記暗号化された第３の暗号化鍵を上記第２の暗号化鍵で復号する復号手段と、

上記記録再生装置に対して伝送するコンテンツ情報を上記第３の暗号化で暗号化する暗号化手段と、

上記暗号化されたコンテンツ情報を上記セッションキーでバス暗号化して上記記録再生装置に送出するバス暗号化手段とを有する信号処理システム。

6．請求の範囲５において、

上記記録再生装置の上記認証手段と上記情報処理装置の上記認証手段とは、生成した乱数データを交換する時に、上記記録再生装置から上記情報処理装置に伝送する乱数に上記記録媒体の種類の情報を混合するようにした信号処理システム。

7．請求の範囲５において、

上記記録再生装置の上記認証手段と上記情報処理装置の上記認証手段とは、生成した乱数データを交換する時に、上記情報処理装置から上記記録再生装置に伝送する乱数に著作権関連情報を混合するようにした信号処理システム。

8．請求の範囲５において、

さらに、暗号化された上記第３の暗号化鍵に対する第１のマスク制御手段と、暗号化された上記第２の暗号化鍵に対する第２のマスク制御手段とを有し、

上記認証手段によって認証が成立している期間のみ、暗号化された上記第３の暗号化鍵および暗号化された上記第２の暗号化鍵の上記記録媒体に対する書き込みが可能とされた信号処理システム。

9．記録媒体から情報を読み出し、記録媒体に情報を記録する記録再生装置と、上記記録再生装置が伝達手段を介して接続される情報処理装置とを備え、管理機構が管理する第１の暗号化鍵と、記録媒体固有の第２の暗号化鍵と、記録の度に生成される第３の暗号化鍵とを使用したコンテンツ情報暗号化方法で暗号化されたコンテンツ情報を記録媒体に記録する信号処理システムであって、

上記記録再生装置は、

第１の暗号化鍵を保持する保持手段と、

記録媒体に暗号化されて記録されている第２の暗号化鍵を再生し、上

記第１の暗号化鍵で復号する第２の暗号化鍵復号手段と、

第３の暗号化鍵を生成する第３の暗号化鍵生成手段と、

第３の暗号化鍵を復号された第２の暗号化鍵で暗号化する暗号化手段と、

情報処理装置との間の認証を行い、認証成立時にセッションキーを生成する認証手段と、

上記情報処理装置からのバス暗号化されたコンテンツ情報をバス復号するバス復号手段と、

上記コンテンツ情報を上記第３の暗号化鍵によって暗号化する暗号化手段と、

上記暗号化された上記第３の暗号化鍵と、上記暗号化されたコンテンツ情報を記録媒体に記録する記録手段とを有し、

上記情報処理装置は、

上記記録再生装置との間の認証を行い、認証成立時にセッションキーを生成する認証手段と、

上記記録再生装置に対して伝送するコンテンツ情報を上記セッションキーでバス暗号化して上記記録再生装置に送出するバス暗号化手段とを有する信号処理システム。

１０．請求の範囲９において、

上記記録再生装置の上記認証手段と上記情報処理装置の上記認証手段とは、生成した乱数データを交換する時に、上記記録再生装置から上記情報処理装置に伝送する乱数に上記記録媒体の種類の情報を混合するようにした信号処理システム。

１１．請求の範囲９において、

上記記録再生装置の上記認証手段と上記情報処理装置の上記認証手段とは、生成した乱数データを交換する時に、上記情報処理装置から上記

記録再生装置に伝送する乱数に著作権関連情報を混合するようにした信号処理システム。

１２．請求の範囲９において、

さらに、暗号化された上記第３の暗号化鍵に対するマスク制御手段を有し、

上記認証手段によって認証が成立している期間のみ、暗号化された上記第３の暗号化鍵の上記記録媒体に対する書き込みが可能とされた信号処理システム。

１３．記録媒体から情報を読み出し、記録媒体に情報を記録する記録再生装置と、上記記録再生装置が伝達手段を介して接続される情報処理装置とを備え、管理機構が管理する第１の暗号化鍵と、記録媒体固有の第２の暗号化鍵と、記録の度に生成される第３の暗号化鍵とを使用したコンテンツ情報暗号化方法で暗号化されたコンテンツ情報を記録媒体に記録する信号処理システムであって、

上記記録再生装置は、

第１の暗号化鍵を保持する保持手段と、

第２の暗号化鍵を生成する第２の暗号化鍵生成手段と、

生成された第２の暗号化鍵を上記第１の暗号化鍵で暗号化する暗号化手段と、

第３の暗号化鍵を生成する第３の暗号化鍵生成手段と、

上記第３の暗号化鍵を生成された第２の暗号化鍵で暗号化する暗号化手段と、

情報処理装置との間の認証を行い、認証成立時にセッションキーを生成する認証手段と、

上記情報処理装置からのバス暗号化されたコンテンツ情報をバス復号するバス復号手段と、

上記コンテンツ情報を上記第３の暗号化鍵によって暗号化する暗号化手段と、

上記暗号化された上記第２の暗号化鍵と、上記暗号化された上記第３の暗号化鍵と、上記暗号化されたコンテンツ情報を記録媒体に記録する記録手段とを有し、

上記情報処理装置は、

上記記録再生装置との間の認証を行い、認証成立時にセッションキーを生成する認証手段と、

コンテンツ情報を上記セッションキーでバス暗号化して上記記録再生装置に送出するバス暗号化手段とを有する信号処理システム。

１４．請求の範囲１３において、

上記記録再生装置の上記認証手段と上記情報処理装置の上記認証手段とは、生成した乱数データを交換する時に、上記記録再生装置から上記情報処理装置に伝送する乱数に上記記録媒体の種類の情報を混合するようにした信号処理システム。

１５．請求の範囲１３において、

上記記録再生装置の上記認証手段と上記情報処理装置の上記認証手段とは、生成した乱数データを交換する時に、上記情報処理装置から上記記録再生装置に伝送する乱数に著作権関連情報を混合するようにした信号処理システム。

１６．請求の範囲１３において、

さらに、暗号化された上記第３の暗号化鍵に対する第１のマスク制御手段と、暗号化された上記第２の暗号化鍵に対する第２のマスク制御手段とを有し、

上記認証手段によって認証が成立している期間のみ、暗号化された上記第３の暗号化鍵および暗号化された上記第２の暗号化鍵の上記記録媒

体に対する書き込みが可能とされた信号処理システム。

１７．伝達手段を介して情報処理装置と接続され、記録媒体から情報を読み出し、記録媒体に情報を記録する記録再生装置であって、管理機構が管理する第１の暗号化鍵と、記録媒体固有の第２の暗号化鍵と、記録の度に生成される第３の暗号化鍵とを使用したコンテンツ情報暗号化方法で暗号化されたコンテンツ情報を記録媒体に記録する記録再生装置であって、

第１の暗号化鍵を保持する保持手段と、

記録媒体に暗号化されて記録されている第２の暗号化鍵を再生し、上記第１の暗号化鍵で復号する第２の暗号化鍵復号手段と、

第３の暗号化鍵を生成する第３の暗号化鍵生成手段と、

上記第３の暗号化鍵を復号された第２の暗号化鍵で暗号化する暗号化手段と、

情報処理装置との間の認証を行い、認証成立時にセッションキーを生成する認証手段と、

上記暗号化されて記録されている第２の暗号化鍵を上記セッションキーによってバス暗号化して上記情報処理装置に伝送する第１のバス暗号化手段と、

暗号化された上記第３の暗号化鍵を上記セッションキーによってバス暗号化して上記情報処理装置に伝送する第２のバス暗号化手段と、

上記情報処理装置からの暗号化およびバス暗号化されたコンテンツ情報をバス復号するバス復号手段と、

上記暗号化された上記第３の暗号化鍵と、上記暗号化されたコンテンツ情報を記録媒体に記録する記録手段とを有し、

上記暗号化およびバス暗号化されたコンテンツ情報は、上記第３の暗号化鍵で暗号化され、さらに、暗号化コンテンツ情報を情報処理装置で

生成されたセッションキーでバス暗号化したものである記録再生装置。

１８．請求の範囲１７において、

上記認証手段は、生成した乱数データを交換する時に、上記情報処理装置に伝送する乱数に上記記録媒体の種類の情報を混合するようにした記録再生装置。

１９．請求の範囲１７において、

さらに、暗号化された上記第３の暗号化鍵に対するマスク制御手段を有し、

上記認証手段によって認証が成立している期間のみ、暗号化された上記第３の暗号化鍵の上記記録媒体に対する書き込みが可能とされた記録再生装置。

２０．伝達手段を介して情報処理装置と接続され、記録媒体から情報を読み出し、記録媒体に情報を記録する記録再生装置であって、管理機構が管理する第１の暗号化鍵と、記録媒体固有の第２の暗号化鍵と、記録の度に生成される第３の暗号化鍵とを使用したコンテンツ情報暗号化方法で暗号化されたコンテンツ情報を記録媒体に記録する記録再生装置であって、

第１の暗号化鍵を保持する保持手段と、

第２の暗号化鍵を生成する第２の暗号化鍵生成手段と、

生成された第２の暗号化鍵を第１の暗号化鍵で暗号化する暗号化手段と、

第３の暗号化鍵を生成する第３の暗号化鍵生成手段と、

生成された第２の暗号化鍵で上記第３の暗号化鍵を暗号化する暗号化手段と、

情報処理装置との間の認証を行い、認証成立時にセッションキーを生成する認証手段と、

上記暗号化された第２の暗号化鍵を上記セッションキーによってバス暗号化して上記情報処理装置に伝送する第１のバス暗号化手段と、

暗号化された上記第３の暗号化鍵を上記セッションキーによってバス暗号化して上記情報処理装置に伝送する第２のバス暗号化手段と、

上記情報処理装置からの暗号化およびバス暗号化されたコンテンツ情報をバス復号するバス復号手段と、

上記暗号化された上記第２の暗号化鍵と、上記暗号化された上記第３の暗号化鍵と、上記暗号化されたコンテンツ情報を記録媒体に記録する記録手段とを有し、

上記暗号化およびバス暗号化されたコンテンツ情報は、上記第３の暗号化鍵で暗号化され、さらに、暗号化コンテンツ情報を情報処理装置で生成されたセッションキーでバス暗号化したものである記録再生装置。

２１．請求の範囲２０において、

上記認証手段は、生成した乱数データを交換する時に、上記情報処理装置に伝送する乱数に上記記録媒体の種類の情報を混合するようにした記録再生装置。

２２．請求の範囲２０において、

さらに、暗号化された上記第３の暗号化鍵に対する第１のマスク制御手段と、暗号化された上記第２の暗号化鍵に対する第２のマスク制御手段とを有し、

上記認証手段によって認証が成立している期間のみ、暗号化された上記第３の暗号化鍵および暗号化された上記第２の暗号化鍵の上記記録媒体に対する書き込みが可能とされた記録再生装置。

２３．伝達手段を介して情報処理装置と接続され、記録媒体から情報を読み出し、記録媒体に情報を記録する記録再生装置であって、管理機構が管理する第１の暗号化鍵と、記録媒体固有の第２の暗号化鍵と、記録

の度に生成される第３の暗号化鍵とを使用したコンテンツ情報暗号化方法で暗号化されたコンテンツ情報を記録媒体に記録する記録再生装置であって、

第１の暗号化鍵を保持する保持手段と、

記録媒体に暗号化されて記録されている第２の暗号化鍵を再生し、上記第１の暗号化鍵で復号する第２の暗号化鍵復号手段と、

第３の暗号化鍵を生成する第３の暗号化鍵生成手段と、

第３の暗号化鍵を復号された第２の暗号化鍵で暗号化する暗号化手段と、

情報処理装置との間の認証を行い、認証成立時にセッションキーを生成する認証手段と、

上記情報処理装置からのバス暗号化されたコンテンツ情報をバス復号するバス復号手段と、

上記コンテンツ情報を上記第３の暗号化鍵によって暗号化する暗号化手段と、

上記暗号化された上記第３の暗号化鍵と、上記暗号化されたコンテンツ情報を記録媒体に記録する記録手段とを有し、

上記バス暗号化されたコンテンツ情報は、暗号化コンテンツ情報を情報処理装置で生成されたセッションキーでバス暗号化したものである記録再生装置。

２４．請求の範囲２３において、

上記認証手段は、生成した乱数データを交換する時に、上記情報処理装置に伝送する乱数に上記記録媒体の種類の情報を混合するようにした記録再生装置。

２５．請求の範囲２３において、

さらに、暗号化された上記第３の暗号化鍵に対するマスク制御手段を

有し、

上記認証手段によって認証が成立している期間のみ、暗号化された上記第３の暗号化鍵の上記記録媒体に対する書き込みが可能とされた記録再生装置。

２６．伝達手段を介して情報処理装置と接続され、記録媒体から情報を読み出し、記録媒体に情報を記録する記録再生装置であって、管理機構が管理する第１の暗号化鍵と、記録媒体固有の第２の暗号化鍵と、記録の度に生成される第３の暗号化鍵とを使用したコンテンツ情報暗号化方法で暗号化されたコンテンツ情報を記録媒体に記録する記録再生装置であって、

第１の暗号化鍵を保持する保持手段と、

第２の暗号化鍵を生成する第２の暗号化鍵生成手段と、

生成された第２の暗号化鍵を上記第１の暗号化鍵で暗号化する暗号化手段と、

第３の暗号化鍵を生成する第３の暗号化鍵生成手段と、

上記第３の暗号化鍵を生成された第２の暗号化鍵で暗号化する暗号化手段と、

情報処理装置との間の認証を行い、認証成立時にセッションキーを生成する認証手段と、

上記情報処理装置からのバス暗号化されたコンテンツ情報をバス復号するバス復号手段と、

上記コンテンツ情報を上記第３の暗号化鍵によって暗号化する暗号化手段と、

上記暗号化された上記第２の暗号化鍵と、上記暗号化された上記第３の暗号化鍵と、上記暗号化されたコンテンツ情報を記録媒体に記録する記録手段とを有し、

上記バス暗号化されたコンテンツ情報は、暗号化コンテンツ情報を情報処理装置で生成されたセッションキーでバス暗号化したものである記録再生装置。

２７．請求の範囲２６において、

上記認証手段は、生成した乱数データを交換する時に、上記情報処理装置に伝送する乱数に上記記録媒体の種類の情報を混合するようにした記録再生装置。

２８．請求の範囲２６において、

さらに、暗号化された上記第３の暗号化鍵に対する第１のマスク制御手段と、暗号化された上記第２の暗号化鍵に対する第２のマスク制御手段とを有し、

上記認証手段によって認証が成立している期間のみ、暗号化された上記第３の暗号化鍵および暗号化された上記第２の暗号化鍵の上記記録媒体に対する書き込みが可能とされた記録再生装置。

２９．記録媒体から情報を読み出し、記録媒体に情報を記録する記録再生装置と、上記記録再生装置が伝達ステップを介して接続される情報処理装置とを備え、管理機構が管理する第１の暗号化鍵と、記録媒体固有の第２の暗号化鍵と、記録の度に生成される第３の暗号化鍵とを使用したコンテンツ情報暗号化方法で暗号化されたコンテンツ情報を記録媒体に記録する記録方法であって、

上記記録再生装置は、

第１の暗号化鍵を保持する保持ステップと、

記録媒体に暗号化されて記録されている第２の暗号化鍵を再生し、上記第１の暗号化鍵で復号する第２の暗号化鍵復号ステップと、

第３の暗号化鍵を生成する第３の暗号化鍵生成ステップと、

上記第３の暗号化鍵を復号された第２の暗号化鍵で暗号化する暗号化

ステップと、

情報処理装置との間の認証を行い、認証成立時にセッションキーを生成する認証ステップと、

上記暗号化されて記録されている第２の暗号化鍵を上記セッションキーによってバス暗号化して上記情報処理装置に伝送する第１のバス暗号化ステップと、

暗号化された上記第３の暗号化鍵を上記セッションキーによってバス暗号化して上記情報処理装置に伝送する第２のバス暗号化ステップと、

上記情報処理装置からの暗号化およびバス暗号化されたコンテンツ情報をバス復号するバス復号ステップと、

上記暗号化された上記第３の暗号化鍵と、上記暗号化されたコンテンツ情報を記録媒体に記録する記録ステップとを実行し、

上記情報処理装置は、

第１の暗号化鍵を保持する保持ステップと、

上記記録再生装置との間の認証を行い、認証成立時にセッションキーを生成する認証ステップと、

上記バス暗号化された第２の暗号化鍵を上記セッションキーによってバス復号して暗号化された上記第２の暗号化鍵を復号する第１のバス復号ステップと、

上記暗号化された第２の暗号化鍵を上記第１の暗号化鍵で復号する復号ステップと、

上記バス暗号化された第３の暗号化鍵を上記セッションキーによってバス復号して上記暗号化された第３の暗号化鍵を復号する第２のバス復号化ステップと、

上記暗号化された第３の暗号化鍵を上記第２の暗号化鍵で復号する復号ステップと、

上記記録再生装置に対して伝送するコンテンツ情報を上記第３の暗号化で暗号化する暗号化ステップと、

上記暗号化されたコンテンツ情報を上記セッションキーでバス暗号化して上記記録再生装置に送出するバス暗号化ステップとを実行する記録方法。

３０．請求の範囲２９において、

上記記録再生装置の上記認証ステップと上記情報処理装置の上記認証ステップとは、生成した乱数データを交換する時に、上記記録再生装置から上記情報処理装置に伝送する乱数に上記記録媒体の種類の情報を混合するようにした記録方法。

３１．請求の範囲２９において、

上記記録再生装置の上記認証ステップと上記情報処理装置の上記認証ステップとは、生成した乱数データを交換する時に、上記情報処理装置から上記記録再生装置に伝送する乱数に著作権関連情報を混合するようにした記録方法。

３２．請求の範囲２９において、

さらに、暗号化された上記第３の暗号化鍵に対するマスク制御ステップを有し、

上記認証ステップによって認証が成立している期間のみ、暗号化された上記第３の暗号化鍵の上記記録媒体に対する書き込みが可能とされた記録方法。

３３．記録媒体から情報を読み出し、記録媒体に情報を記録する記録再生装置と、上記記録再生装置が伝達ステップを介して接続される情報処理装置とを備え、管理機構が管理する第１の暗号化鍵と、記録媒体固有の第２の暗号化鍵と、記録の度に生成される第３の暗号化鍵とを使用したコンテンツ情報暗号化方法で暗号化されたコンテンツ情報を記録媒体

に記録する記録方法であって、

上記記録再生装置は、

第１の暗号化鍵を保持する保持ステップと、

第２の暗号化鍵を生成する第２の暗号化鍵生成ステップと、

生成された第２の暗号化鍵を第１の暗号化鍵で暗号化する暗号化ステップと、

第３の暗号化鍵を生成する第３の暗号化鍵生成ステップと、

生成された第２の暗号化鍵で上記第３の暗号化鍵を暗号化する暗号化ステップと、

情報処理装置との間の認証を行い、認証成立時にセッションキーを生成する認証ステップと、

上記暗号化された第２の暗号化鍵を上記セッションキーによってバス暗号化して上記情報処理装置に伝送する第１のバス暗号化ステップと、

暗号化された上記第３の暗号化鍵を上記セッションキーによってバス暗号化して上記情報処理装置に伝送する第２のバス暗号化ステップと、

上記情報処理装置からの暗号化およびバス暗号化されたコンテンツ情報をバス復号するバス復号ステップと、

上記暗号化された上記第２の暗号化鍵と、上記暗号化された上記第３の暗号化鍵と、上記暗号化されたコンテンツ情報を記録媒体に記録する記録ステップとを実行し、

上記情報処理装置は、

第１の暗号化鍵を保持する保持ステップと、

上記記録再生装置との間の認証を行い、認証成立時にセッションキーを生成する認証ステップと、

上記バス暗号化された第２の暗号化鍵を上記セッションキーによってバス復号して暗号化された上記第２の暗号化鍵を復号する第１のバス復

号ステップと、

上記暗号化された第２の暗号化鍵を上記第１の暗号化鍵で復号する復号ステップと、

上記バス暗号化された第３の暗号化鍵を上記セッションキーによってバス復号して上記暗号化された第３の暗号化鍵を復号する第２のバス復号化ステップと、

上記暗号化された第３の暗号化鍵を上記第２の暗号化鍵で復号する復号ステップと、

上記記録再生装置に対して伝送するコンテンツ情報を上記第３の暗号化で暗号化する暗号化ステップと、

上記暗号化されたコンテンツ情報を上記セッションキーでバス暗号化して上記記録再生装置に送出するバス暗号化ステップとを実行する記録方法。

３４．請求の範囲３３において、

上記記録再生装置の上記認証ステップと上記情報処理装置の上記認証ステップとは、生成した乱数データを交換する時に、上記記録再生装置から上記情報処理装置に伝送する乱数に上記記録媒体の種類の情報を混合するようにした記録方法。

３５．請求の範囲３３において、

上記記録再生装置の上記認証ステップと上記情報処理装置の上記認証ステップとは、生成した乱数データを交換する時に、上記情報処理装置から上記記録再生装置に伝送する乱数に著作権関連情報を混合するようにした記録方法。

３６．請求の範囲３３において、

さらに、暗号化された上記第３の暗号化鍵に対する第１のマスク制御ステップと、暗号化された上記第２の暗号化鍵に対する第２のマスク制

御ステップとを有し、

上記認証ステップによって認証が成立している期間のみ、暗号化された上記第３の暗号化鍵および暗号化された上記第２の暗号化鍵の上記記録媒体に対する書き込みが可能とされた記録方法。

３７．記録媒体から情報を読み出し、記録媒体に情報を記録する記録再生装置と、上記記録再生装置が伝達ステップを介して接続される情報処理装置とを備え、管理機構が管理する第１の暗号化鍵と、記録媒体固有の第２の暗号化鍵と、記録の度に生成される第３の暗号化鍵とを使用したコンテンツ情報暗号化方法で暗号化されたコンテンツ情報を記録媒体に記録する記録方法であって、

上記記録再生装置は、

第１の暗号化鍵を保持する保持ステップと、

記録媒体に暗号化されて記録されている第２の暗号化鍵を再生し、上記第１の暗号化鍵で復号する第２の暗号化鍵復号ステップと、

第３の暗号化鍵を生成する第３の暗号化鍵生成ステップと、

第３の暗号化鍵を復号された第２の暗号化鍵で暗号化する暗号化ステップと、

情報処理装置との間の認証を行い、認証成立時にセッションキーを生成する認証ステップと、

上記情報処理装置からのバス暗号化されたコンテンツ情報をバス復号するバス復号ステップと、

上記コンテンツ情報を上記第３の暗号化鍵によって暗号化する暗号化ステップと、

上記暗号化された上記第３の暗号化鍵と、上記暗号化されたコンテンツ情報を記録媒体に記録する記録ステップとを実行し、

上記情報処理装置は、

上記記録再生装置との間の認証を行い、認証成立時にセッションキーを生成する認証ステップと、

上記記録再生装置に対して伝送するコンテンツ情報を上記セッションキーでバス暗号化して上記記録再生装置に送出するバス暗号化ステップとを実行する記録方法。

３８．請求の範囲３７において、

上記記録再生装置の上記認証ステップと上記情報処理装置の上記認証ステップとは、生成した乱数データを交換する時に、上記記録再生装置から上記情報処理装置に伝送する乱数に上記記録媒体の種類の情報を混合するようにした記録方法。

３９．請求の範囲３７において、

上記記録再生装置の上記認証ステップと上記情報処理装置の上記認証ステップとは、生成した乱数データを交換する時に、上記情報処理装置から上記記録再生装置に伝送する乱数に著作権関連情報を混合するようにした記録方法。

４０．請求の範囲３７において、

さらに、暗号化された上記第３の暗号化鍵に対するマスク制御ステップを有し、

上記認証ステップによって認証が成立している期間のみ、暗号化された上記第３の暗号化鍵の上記記録媒体に対する書き込みが可能とされた記録方法。

４１．記録媒体から情報を読み出し、記録媒体に情報を記録する記録再生装置と、上記記録再生装置が伝達ステップを介して接続される情報処理装置とを備え、管理機構が管理する第１の暗号化鍵と、記録媒体固有の第２の暗号化鍵と、記録の度に生成される第３の暗号化鍵とを使用したコンテンツ情報暗号化方法で暗号化されたコンテンツ情報を記録媒体

に記録する記録方法であって、

上記記録再生装置は、

第１の暗号化鍵を保持する保持ステップと、

第２の暗号化鍵を生成する第２の暗号化鍵生成ステップと、

生成された第２の暗号化鍵を上記第１の暗号化鍵で暗号化する暗号化ステップと、

第３の暗号化鍵を生成する第３の暗号化鍵生成ステップと、

上記第３の暗号化鍵を生成された第２の暗号化鍵で暗号化する暗号化ステップと、

情報処理装置との間の認証を行い、認証成立時にセッションキーを生成する認証ステップと、

上記情報処理装置からのバス暗号化されたコンテンツ情報をバス復号するバス復号ステップと、

上記コンテンツ情報を上記第３の暗号化鍵によって暗号化する暗号化ステップと、

上記暗号化された上記第２の暗号化鍵と、上記暗号化された上記第３の暗号化鍵と、上記暗号化されたコンテンツ情報を記録媒体に記録する記録ステップとを実行し、

上記情報処理装置は、

上記記録再生装置との間の認証を行い、認証成立時にセッションキーを生成する認証ステップと、

コンテンツ情報を上記セッションキーでバス暗号化して上記記録再生装置に送出するバス暗号化ステップとを実行する記録方法。

４２．請求の範囲４１において、

上記記録再生装置の上記認証ステップと上記情報処理装置の上記認証ステップとは、生成した乱数データを交換する時に、上記記録再生装置

から上記情報処理装置に伝送する乱数に上記記録媒体の種類の情報を混合するようにした記録方法。

４３．請求の範囲４１において、

上記記録再生装置の上記認証ステップと上記情報処理装置の上記認証ステップとは、生成した乱数データを交換する時に、上記情報処理装置から上記記録再生装置に伝送する乱数に著作権関連情報を混合するようにした記録方法。

４４．請求の範囲４１において、

さらに、暗号化された上記第３の暗号化鍵に対する第１のマスク制御ステップと、暗号化された上記第２の暗号化鍵に対する第２のマスク制御ステップとを有し、

上記認証ステップによって認証が成立している期間のみ、暗号化された上記第３の暗号化鍵および暗号化された上記第２の暗号化鍵の上記記録媒体に対する書き込みが可能とされた記録方法。

４５．記録媒体から情報を読み出し、記録媒体に情報を記録する記録再生装置と、上記記録再生装置が伝達ステップを介して接続される情報処理装置とを備え、管理機構が管理する第１の暗号化鍵と、記録媒体固有の第２の暗号化鍵と、記録の度に生成される第３の暗号化鍵とを使用したコンテンツ情報暗号化方法で暗号化されたコンテンツ情報を記録媒体に記録する記録方法のプログラムであって、

上記記録再生装置に、

第１の暗号化鍵を保持する保持ステップと、

記録媒体に暗号化されて記録されている第２の暗号化鍵を再生し、上記第１の暗号化鍵で復号する第２の暗号化鍵復号ステップと、

第３の暗号化鍵を生成する第３の暗号化鍵生成ステップと、

上記第３の暗号化鍵を復号された第２の暗号化鍵で暗号化する暗号化

ステップと、

情報処理装置との間の認証を行い、認証成立時にセッションキーを生成する認証ステップと、

上記暗号化されて記録されている第２の暗号化鍵を上記セッションキーによってバス暗号化して上記情報処理装置に伝送する第１のバス暗号化ステップと、

暗号化された上記第３の暗号化鍵を上記セッションキーによってバス暗号化して上記情報処理装置に伝送する第２のバス暗号化ステップと、

上記情報処理装置からの暗号化およびバス暗号化されたコンテンツ情報をバス復号するバス復号ステップと、

上記暗号化された上記第３の暗号化鍵と、上記暗号化されたコンテンツ情報を記録媒体に記録する記録ステップとを実行させ、

上記情報処理装置に、

第１の暗号化鍵を保持する保持ステップと、

上記記録再生装置との間の認証を行い、認証成立時にセッションキーを生成する認証ステップと、

上記バス暗号化された第２の暗号化鍵を上記セッションキーによってバス復号して暗号化された上記第２の暗号化鍵を復号する第１のバス復号ステップと、

上記暗号化された第２の暗号化鍵を上記第１の暗号化鍵で復号する復号ステップと、

上記バス暗号化された第３の暗号化鍵を上記セッションキーによってバス復号して上記暗号化された第３の暗号化鍵を復号する第２のバス復号化ステップと、

上記暗号化された第３の暗号化鍵を上記第２の暗号化鍵で復号する復

号ステップと、

上記記録再生装置に対して伝送するコンテンツ情報を上記第３の暗号化で暗号化する暗号化ステップと、

上記暗号化されたコンテンツ情報を上記セッションキーでバス暗号化して上記記録再生装置に送出するバス暗号化ステップとを実行させる記録方法のプログラム。

４６．記録媒体から情報を読み出し、記録媒体に情報を記録する記録再生装置と、上記記録再生装置が伝達ステップを介して接続される情報処理装置とを備え、管理機構が管理する第１の暗号化鍵と、記録媒体固有の第２の暗号化鍵と、記録の度に生成される第３の暗号化鍵とを使用したコンテンツ情報暗号化方法で暗号化されたコンテンツ情報を記録媒体に記録する記録方法のプログラムであって、

上記記録再生装置に、

第１の暗号化鍵を保持する保持ステップと、

第２の暗号化鍵を生成する第２の暗号化鍵生成ステップと、

生成された第２の暗号化鍵を第１の暗号化鍵で暗号化する暗号化ステップと、

第３の暗号化鍵を生成する第３の暗号化鍵生成ステップと、

生成された第２の暗号化鍵で上記第３の暗号化鍵を暗号化する暗号化ステップと、

情報処理装置との間の認証を行い、認証成立時にセッションキーを生成する認証ステップと、

上記暗号化された第２の暗号化鍵を上記セッションキーによってバス暗号化して上記情報処理装置に伝送する第１のバス暗号化ステップと、

暗号化された上記第３の暗号化鍵を上記セッションキーによってバス暗号化して上記情報処理装置に伝送する第２のバス暗号化ステップと、

上記情報処理装置からの暗号化およびバス暗号化されたコンテンツ情報をバス復号するバス復号ステップと、

上記暗号化された上記第２の暗号化鍵と、上記暗号化された上記第３の暗号化鍵と、上記暗号化されたコンテンツ情報を記録媒体に記録する記録ステップとを実行させ、

上記情報処理装置に、

第１の暗号化鍵を保持する保持ステップと、

上記記録再生装置との間の認証を行い、認証成立時にセッションキーを生成する認証ステップと、

上記バス暗号化された第２の暗号化鍵を上記セッションキーによってバス復号して暗号化された上記第２の暗号化鍵を復号する第１のバス復号ステップと、

上記暗号化された第２の暗号化鍵を上記第１の暗号化鍵で復号する復号ステップと、

上記バス暗号化された第３の暗号化鍵を上記セッションキーによってバス復号して上記暗号化された第３の暗号化鍵を復号する第２のバス復号化ステップと、

上記暗号化された第３の暗号化鍵を上記第２の暗号化鍵で復号する復号ステップと、

上記記録再生装置に対して伝送するコンテンツ情報を上記第３の暗号化で暗号化する暗号化ステップと、

上記暗号化されたコンテンツ情報を上記セッションキーでバス暗号化して上記記録再生装置に送出するバス暗号化ステップとを実行させる記録方法のプログラム。

４７．記録媒体から情報を読み出し、記録媒体に情報を記録する記録再生装置と、上記記録再生装置が伝達ステップを介して接続される情報処

理装置とを備え、管理機構が管理する第１の暗号化鍵と、記録媒体固有の第２の暗号化鍵と、記録の度に生成される第３の暗号化鍵とを使用したコンテンツ情報暗号化方法で暗号化されたコンテンツ情報を記録媒体に記録する記録方法のプログラムであって、

上記記録再生装置に、

第１の暗号化鍵を保持する保持ステップと、

記録媒体に暗号化されて記録されている第２の暗号化鍵を再生し、上記第１の暗号化鍵で復号する第２の暗号化鍵復号ステップと、

第３の暗号化鍵を生成する第３の暗号化鍵生成ステップと、

第３の暗号化鍵を復号された第２の暗号化鍵で暗号化する暗号化ステップと、

情報処理装置との間の認証を行い、認証成立時にセッションキーを生成する認証ステップと、

上記情報処理装置からのバス暗号化されたコンテンツ情報をバス復号するバス復号ステップと、

上記コンテンツ情報を上記第３の暗号化鍵によって暗号化する暗号化ステップと、

上記暗号化された上記第３の暗号化鍵と、上記暗号化されたコンテンツ情報を記録媒体に記録する記録ステップとを実行させ、

上記情報処理装置に、

上記記録再生装置との間の認証を行い、認証成立時にセッションキーを生成する認証ステップと、

上記記録再生装置に対して伝送するコンテンツ情報を上記セッションキーでバス暗号化して上記記録再生装置に送出するバス暗号化ステップとを実行させる記録方法のプログラム。

４８．記録媒体から情報を読み出し、記録媒体に情報を記録する記録再

生装置と、上記記録再生装置が伝達ステップを介して接続される情報処理装置とを備え、管理機構が管理する第１の暗号化鍵と、記録媒体固有の第２の暗号化鍵と、記録の度に生成される第３の暗号化鍵とを使用したコンテンツ情報暗号化方法で暗号化されたコンテンツ情報を記録媒体に記録する記録方法のプログラムであって、

上記記録再生装置に、

第１の暗号化鍵を保持する保持ステップと、

第２の暗号化鍵を生成する第２の暗号化鍵生成ステップと、

生成された第２の暗号化鍵を上記第１の暗号化鍵で暗号化する暗号化ステップと、

第３の暗号化鍵を生成する第３の暗号化鍵生成ステップと、

上記第３の暗号化鍵を生成された第２の暗号化鍵で暗号化する暗号化ステップと、

情報処理装置との間の認証を行い、認証成立時にセッションキーを生成する認証ステップと、

上記情報処理装置からのバス暗号化されたコンテンツ情報をバス復号するバス復号ステップと、

上記コンテンツ情報を上記第３の暗号化鍵によって暗号化する暗号化ステップと、

上記暗号化された上記第２の暗号化鍵と、上記暗号化された上記第３の暗号化鍵と、上記暗号化されたコンテンツ情報を記録媒体に記録する記録ステップとを実行させ、

上記情報処理装置に、

上記記録再生装置との間の認証を行い、認証成立時にセッションキーを生成する認証ステップと、

コンテンツ情報を上記セッションキーでバス暗号化して上記記録再生

装置に送出するバス暗号化ステップとを実行させる記録方法のプログラム。

４９．記録媒体から情報を読み出し、記録媒体に情報を記録する記録再生装置と、上記記録再生装置が伝達ステップを介して接続される情報処理装置とを備え、管理機構が管理する第１の暗号化鍵と、記録媒体固有の第２の暗号化鍵と、記録の度に生成される第３の暗号化鍵とを使用したコンテンツ情報暗号化方法で暗号化されたコンテンツ情報を記録媒体に記録する記録方法のプログラムを格納した記録媒体であって、

上記記録再生装置に、

第１の暗号化鍵を保持する保持ステップと、

記録媒体に暗号化されて記録されている第２の暗号化鍵を再生し、上記第１の暗号化鍵で復号する第２の暗号化鍵復号ステップと、

第３の暗号化鍵を生成する第３の暗号化鍵生成ステップと、

上記第３の暗号化鍵を復号された第２の暗号化鍵で暗号化する暗号化ステップと、

情報処理装置との間の認証を行い、認証成立時にセッションキーを生成する認証ステップと、

上記暗号化されて記録されている第２の暗号化鍵を上記セッションキーによってバス暗号化して上記情報処理装置に伝送する第１のバス暗号化ステップと、

暗号化された上記第３の暗号化鍵を上記セッションキーによってバス暗号化して上記情報処理装置に伝送する第２のバス暗号化ステップと、

上記情報処理装置からの暗号化およびバス暗号化されたコンテンツ情報をバス復号するバス復号ステップと、

上記暗号化された上記第３の暗号化鍵と、上記暗号化されたコンテンツ情報を記録媒体に記録する記録ステップとを実行させ、

上記情報処理装置に、

第１の暗号化鍵を保持する保持ステップと、

上記記録再生装置との間の認証を行い、認証成立時にセッションキーを生成する認証ステップと、

上記バス暗号化された第２の暗号化鍵を上記セッションキーによってバス復号して暗号化された上記第２の暗号化鍵を復号する第１のバス復号ステップと、

上記暗号化された第２の暗号化鍵を上記第１の暗号化鍵で復号する復号ステップと、

上記バス暗号化された第３の暗号化鍵を上記セッションキーによってバス復号して上記暗号化された第３の暗号化鍵を復号する第２のバス復号化ステップと、

上記暗号化された第３の暗号化鍵を上記第２の暗号化鍵で復号する復号ステップと、

上記記録再生装置に対して伝送するコンテンツ情報を上記第３の暗号化で暗号化する暗号化ステップと、

上記暗号化されたコンテンツ情報を上記セッションキーでバス暗号化して上記記録再生装置に送出するバス暗号化ステップとを実行させる記録方法のプログラムを格納した記録媒体。

５０．記録媒体から情報を読み出し、記録媒体に情報を記録する記録再生装置と、上記記録再生装置が伝達ステップを介して接続される情報処理装置とを備え、管理機構が管理する第１の暗号化鍵と、記録媒体固有の第２の暗号化鍵と、記録の度に生成される第３の暗号化鍵とを使用したコンテンツ情報暗号化方法で暗号化されたコンテンツ情報を記録媒体に記録する記録方法のプログラムを格納した記録媒体であって、

上記記録再生装置に、

第１の暗号化鍵を保持する保持ステップと、

第２の暗号化鍵を生成する第２の暗号化鍵生成ステップと、

生成された第２の暗号化鍵を第１の暗号化鍵で暗号化する暗号化ステップと、

第３の暗号化鍵を生成する第３の暗号化鍵生成ステップと、

生成された第２の暗号化鍵で上記第３の暗号化鍵を暗号化する暗号化ステップと、

情報処理装置との間の認証を行い、認証成立時にセッションキーを生成する認証ステップと、

上記暗号化された第２の暗号化鍵を上記セッションキーによってバス暗号化して上記情報処理装置に伝送する第１のバス暗号化ステップと、

暗号化された上記第３の暗号化鍵を上記セッションキーによってバス暗号化して上記情報処理装置に伝送する第２のバス暗号化ステップと、

上記情報処理装置からの暗号化およびバス暗号化されたコンテンツ情報をバス復号するバス復号ステップと、

上記暗号化された上記第２の暗号化鍵と、上記暗号化された上記第３の暗号化鍵と、上記暗号化されたコンテンツ情報を記録媒体に記録する記録ステップとを実行させ、

上記情報処理装置に、

第１の暗号化鍵を保持する保持ステップと、

上記記録再生装置との間の認証を行い、認証成立時にセッションキーを生成する認証ステップと、

上記バス暗号化された第２の暗号化鍵を上記セッションキーによってバス復号して暗号化された上記第２の暗号化鍵を復号する第１のバス復号ステップと、

上記暗号化された第２の暗号化鍵を上記第１の暗号化鍵で復号する復

号ステップと、

上記バス暗号化された第３の暗号化鍵を上記セッションキーによってバス復号して上記暗号化された第３の暗号化鍵を復号する第２のバス復号化ステップと、

上記暗号化された第３の暗号化鍵を上記第２の暗号化鍵で復号する復号ステップと、

上記記録再生装置に対して伝送するコンテンツ情報を上記第３の暗号化で暗号化する暗号化ステップと、

上記暗号化されたコンテンツ情報を上記セッションキーでバス暗号化して上記記録再生装置に送出するバス暗号化ステップとを実行させる記録方法のプログラムを格納した記録媒体。

５１．記録媒体から情報を読み出し、記録媒体に情報を記録する記録再生装置と、上記記録再生装置が伝達ステップを介して接続される情報処理装置とを備え、管理機構が管理する第１の暗号化鍵と、記録媒体固有の第２の暗号化鍵と、記録の度に生成される第３の暗号化鍵とを使用したコンテンツ情報暗号化方法で暗号化されたコンテンツ情報を記録媒体に記録する記録方法のプログラムを格納した記録媒体であって、

上記記録再生装置に、

第１の暗号化鍵を保持する保持ステップと、

記録媒体に暗号化されて記録されている第２の暗号化鍵を再生し、上記第１の暗号化鍵で復号する第２の暗号化鍵復号ステップと、

第３の暗号化鍵を生成する第３の暗号化鍵生成ステップと、

第３の暗号化鍵を復号された第２の暗号化鍵で暗号化する暗号化ステップと、

情報処理装置との間の認証を行い、認証成立時にセッションキーを生成する認証ステップと、

上記情報処理装置からのバス暗号化されたコンテンツ情報をバス復号するバス復号ステップと、

上記コンテンツ情報を上記第３の暗号化鍵によって暗号化する暗号化ステップと、

上記暗号化された上記第３の暗号化鍵と、上記暗号化されたコンテンツ情報を記録媒体に記録する記録ステップとを実行させ、

上記情報処理装置に、

上記記録再生装置との間の認証を行い、認証成立時にセッションキーを生成する認証ステップと、

上記記録再生装置に対して伝送するコンテンツ情報を上記セッションキーでバス暗号化して上記記録再生装置に送出するバス暗号化ステップとを実行させる記録方法のプログラムを格納した記録媒体。

５２．記録媒体から情報を読み出し、記録媒体に情報を記録する記録再生装置と、上記記録再生装置が伝達ステップを介して接続される情報処理装置とを備え、管理機構が管理する第１の暗号化鍵と、記録媒体固有の第２の暗号化鍵と、記録の度に生成される第３の暗号化鍵とを使用したコンテンツ情報暗号化方法で暗号化されたコンテンツ情報を記録媒体に記録する記録方法のプログラムを格納した記録媒体であって、

上記記録再生装置に、

第１の暗号化鍵を保持する保持ステップと、

第２の暗号化鍵を生成する第２の暗号化鍵生成ステップと、

生成された第２の暗号化鍵を上記第１の暗号化鍵で暗号化する暗号化ステップと、

第３の暗号化鍵を生成する第３の暗号化鍵生成ステップと、

上記第３の暗号化鍵を生成された第２の暗号化鍵で暗号化する暗号化ステップと、

情報処理装置との間の認証を行い、認証成立時にセッションキーを生成する認証ステップと、

上記情報処理装置からのバス暗号化されたコンテンツ情報をバス復号するバス復号ステップと、

上記コンテンツ情報を上記第３の暗号化鍵によって暗号化する暗号化ステップと、

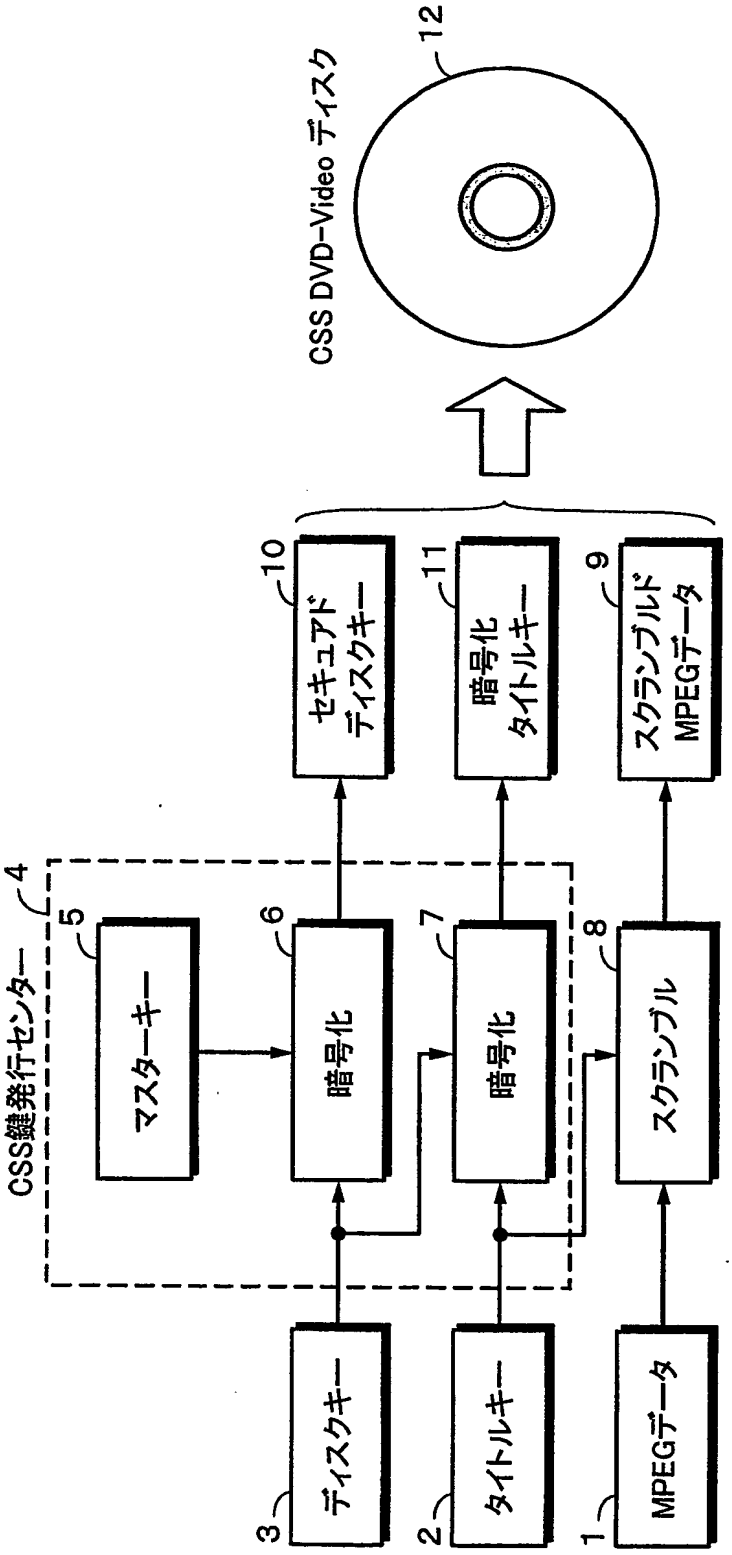
上記暗号化された上記第２の暗号化鍵と、上記暗号化された上記第３の暗号化鍵と、上記暗号化されたコンテンツ情報を記録媒体に記録する記録ステップとを実行させ、

上記情報処理装置に、

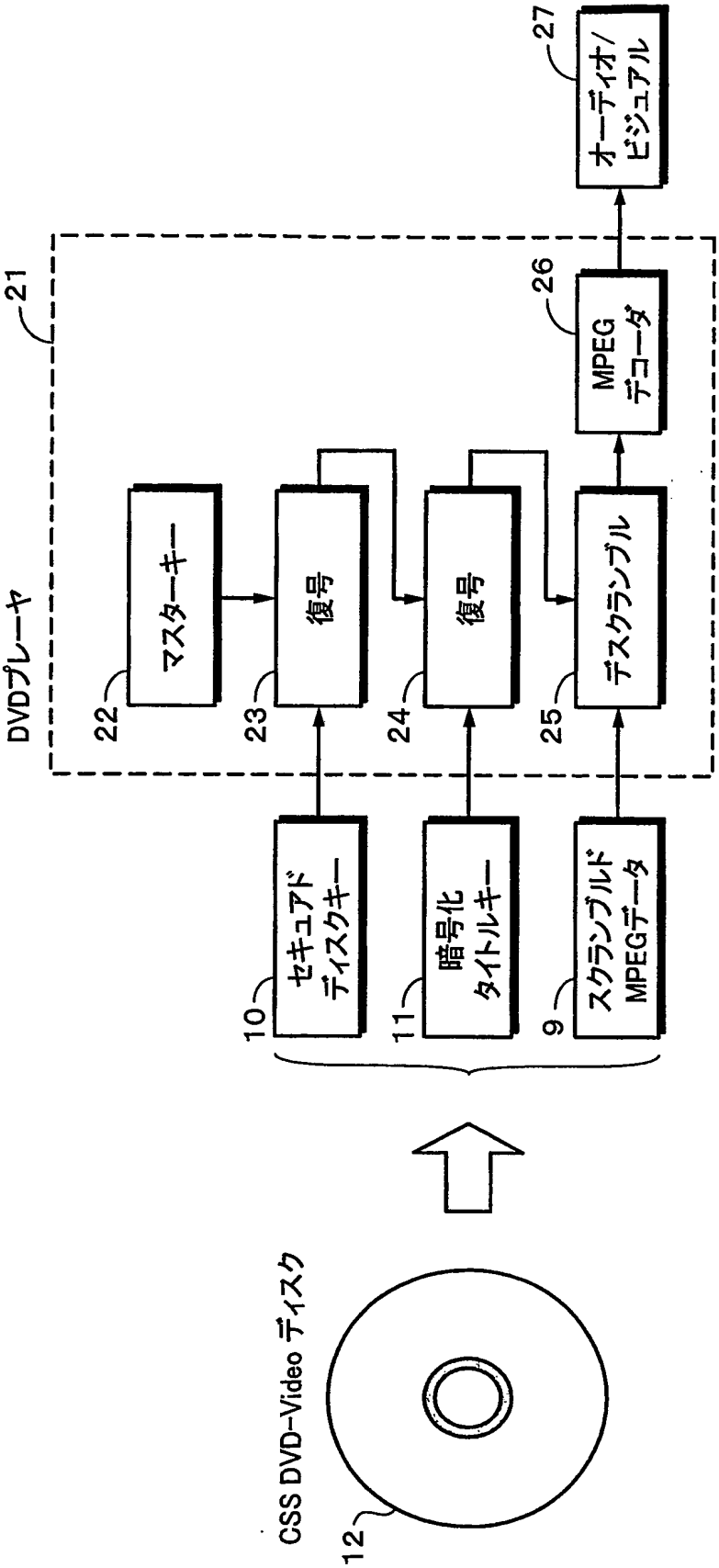
上記記録再生装置との間の認証を行い、認証成立時にセッションキーを生成する認証ステップと、

コンテンツ情報を上記セッションキーでバス暗号化して上記記録再生装置に送出するバス暗号化ステップとを実行させる記録方法のプログラムを格納した記録媒体。

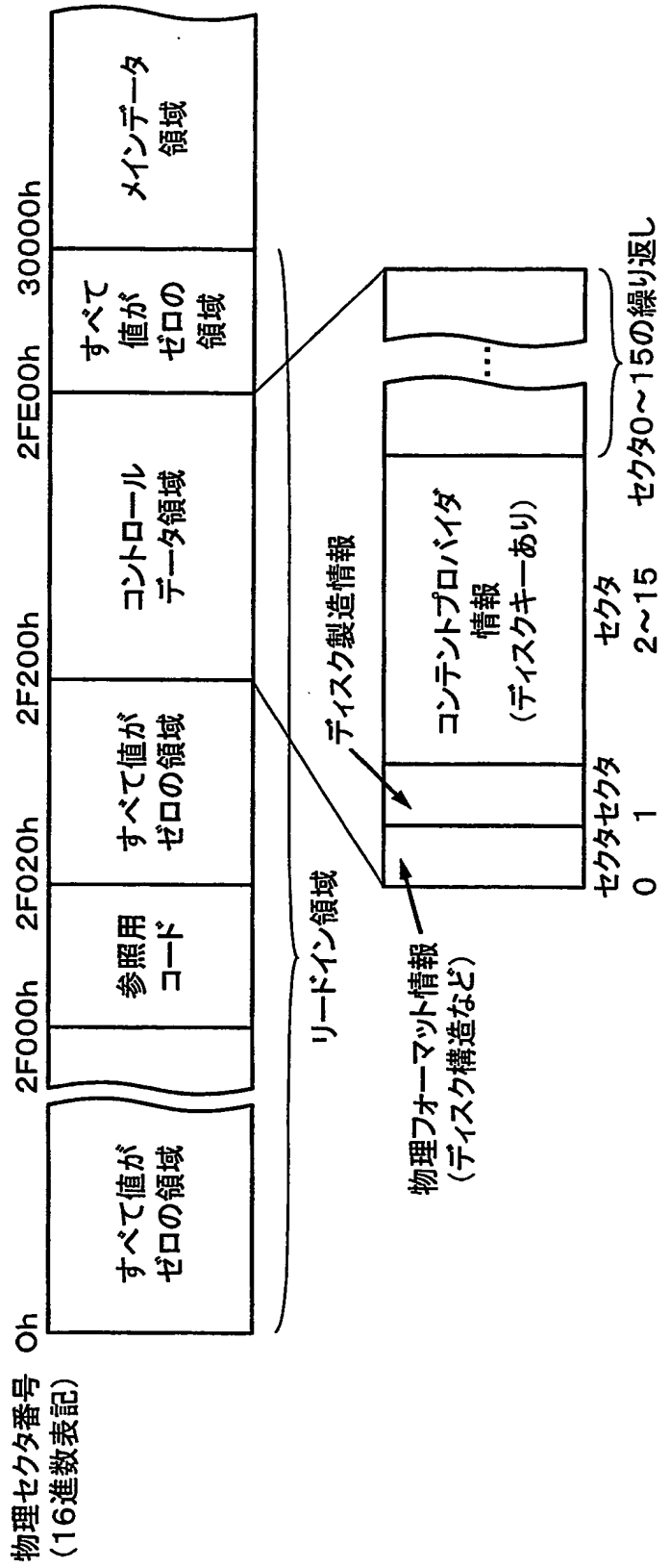
第１図


CSS DVD-Video ディスク
12
セキュアド ディスクキー
10
暗号化 タイトルキー
11
スクランブルド MPEGデータ
9
CSS鍵発行センター
4
マスターキー
5
暗号化
6
暗号化
7
スクランブル
8
ディスクキー
3
タイトルキー
2
MPEGデータ
1

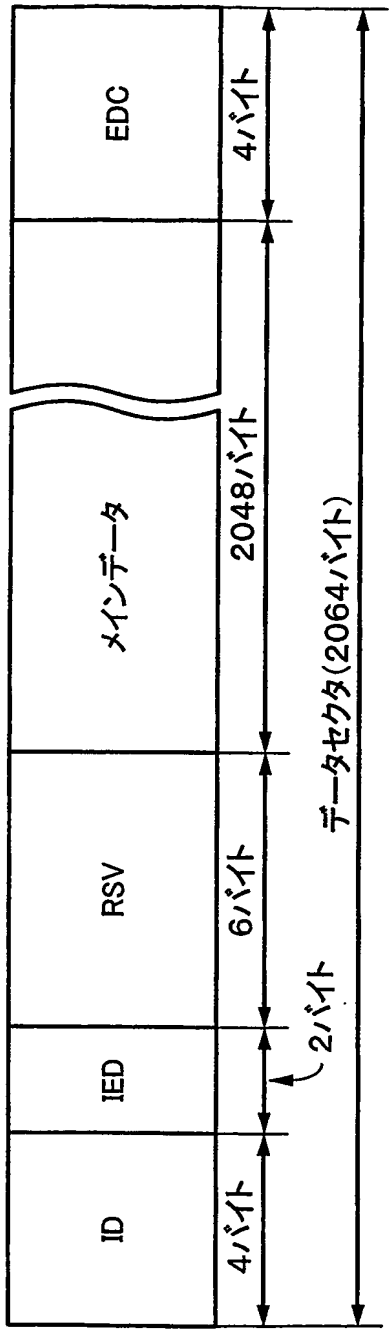
第2図


CSS DVD-Video ディスク
12
セキュアド ディスクキー
10
暗号化 タイトルキー
11
スクランブルド MPEGデータ
9
DVDプレーヤ
21
マスターキー
22
復号
23
復号
24
デスクランブル
25
MPEG デコーダ
26
オーディオ/ ビジュアル
27

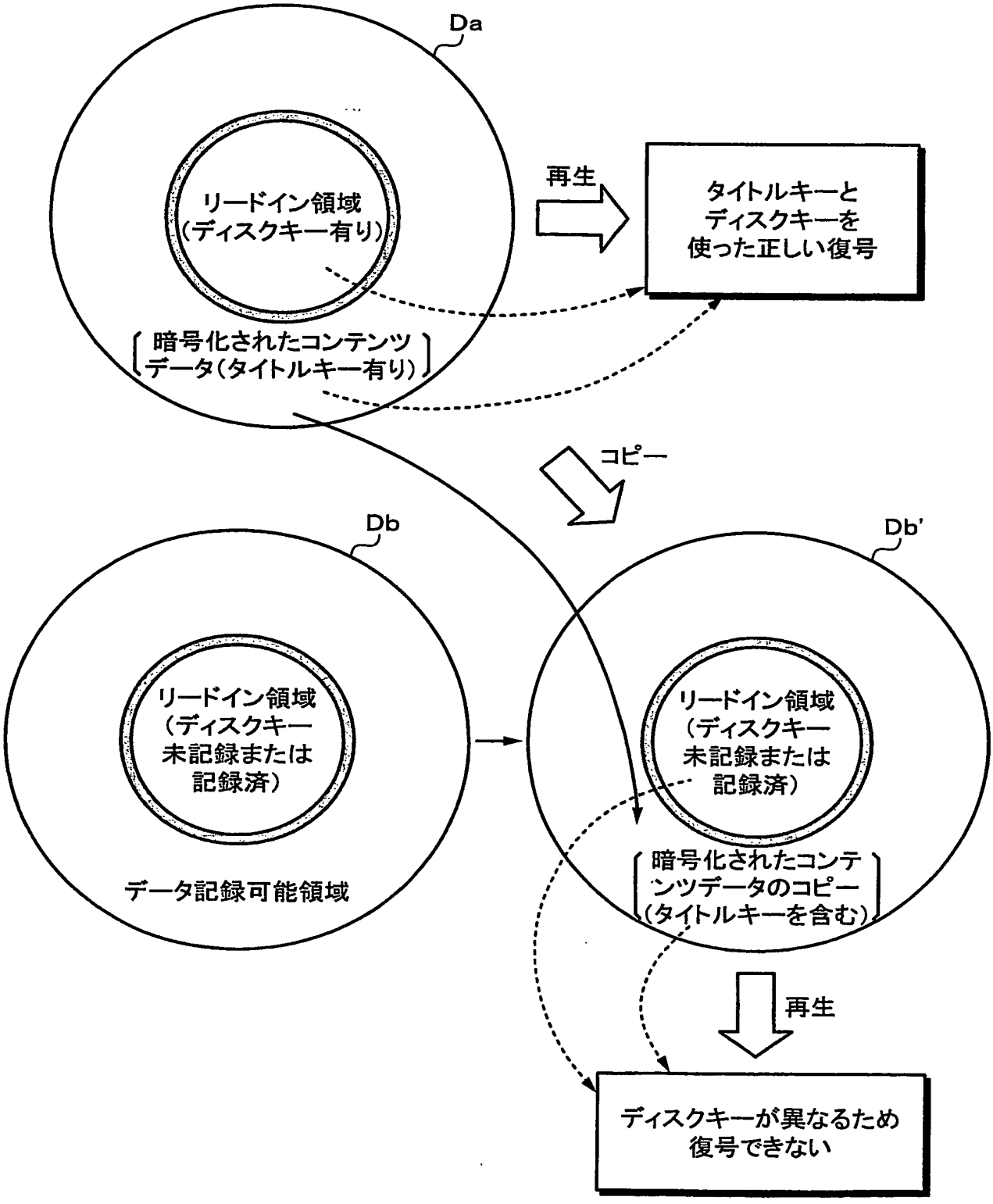
第3図


物理セクタ番号
(16進数表記)
0h
2F000h
2F020h
2F200h
2FE00h
30000h
すべて値が
ゼロの領域
参照用
コード
すべて値が
ゼロの領域
コントロール
データ領域
すべて
値が
ゼロの
領域
メインデータ
領域
リードイン領域
ディスク製造情報
物理フォーマット情報
(ディスク構造など)
コンテントプロバイダ
情報
(ディスクキーあり)
セクタ
2~15
セクタ0~15の繰り返し
セクタセクタ
0 1

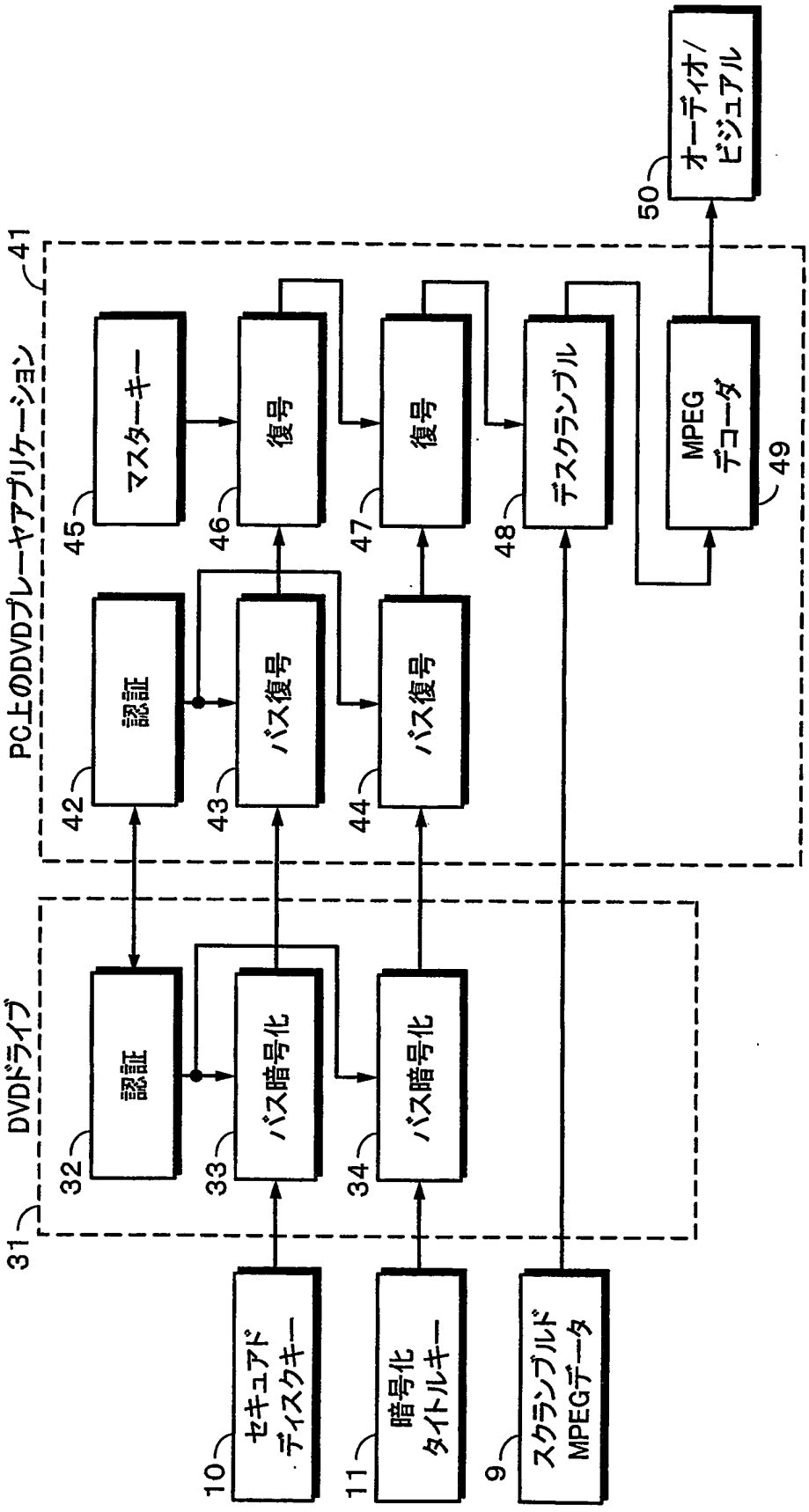
第４図


ID
IED
RSV
メインデータ
EDC
4バイト
2バイト
6バイト
2048バイト
4バイト
データセクタ(2064バイト)

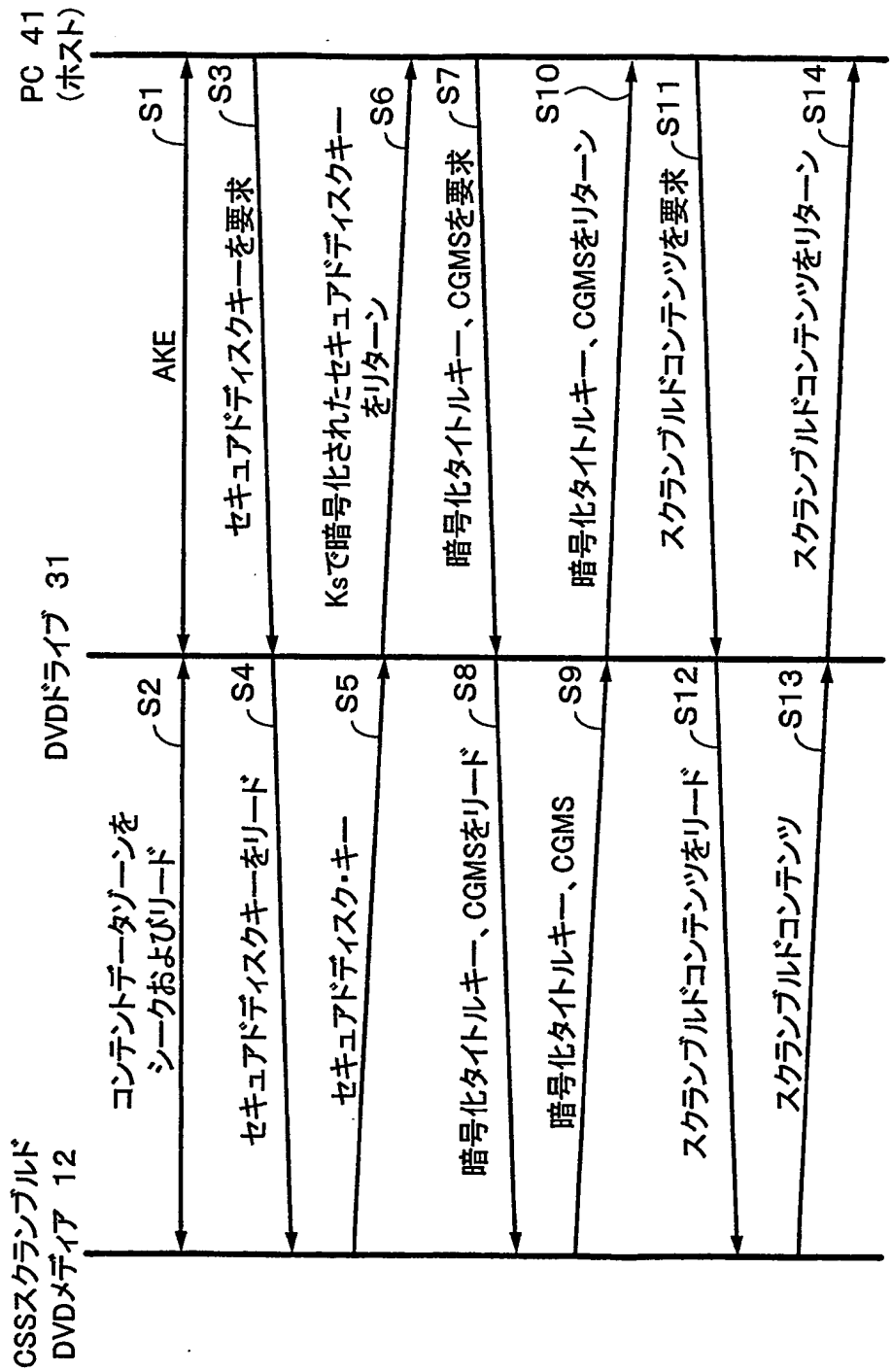
第５図


Da
リードイン領域
(ディスクキー有り)
再生
タイトルキーと
ディスクキーを
使った正しい復号
暗号化されたコンテンツ
データ(タイトルキー有り)
コピー
Db
Db'
リードイン領域
(ディスクキー
未記録または
記録済)
リードイン領域
(ディスクキー
未記録または
記録済)
データ記録可能領域
暗号化されたコンテ
ンツデータのコピー
(タイトルキーを含む)
再生
ディスクキーが異なるため
復号できない

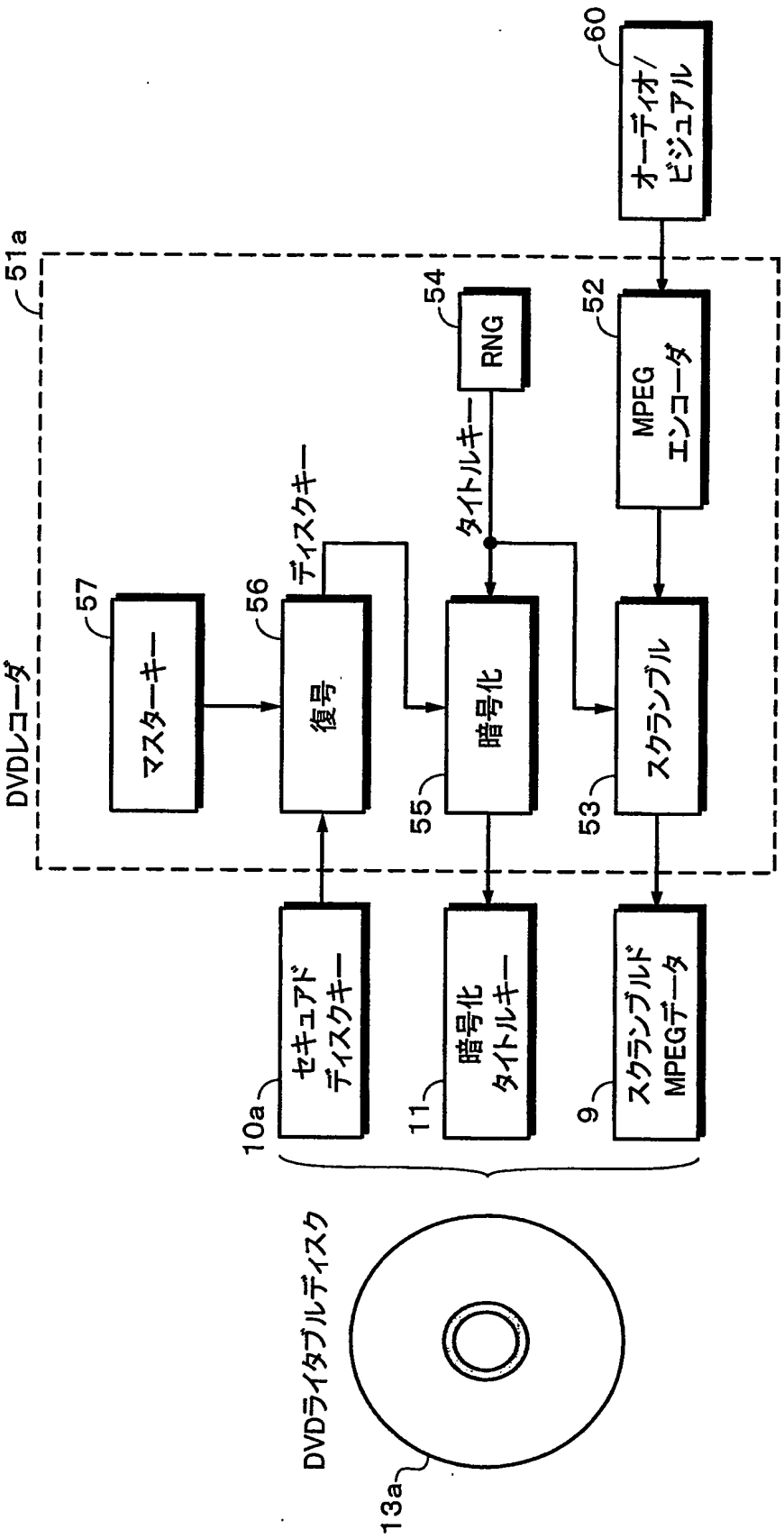
第6図


PC上のDVDプレーヤアプリケーション
41
DVDドライブ
31
マスターキー
45
復号
46
復号
47
デスクランブル
48
MPEG
デコーダ
49
オーディオ/
ビジュアル
50
認証
42
バス復号
43
バス復号
44
認証
32
バス暗号化
33
バス暗号化
34
セキュアド
ディスクキー
10
暗号化
タイトルキー
11
スクランブルド
MPEGデータ
9

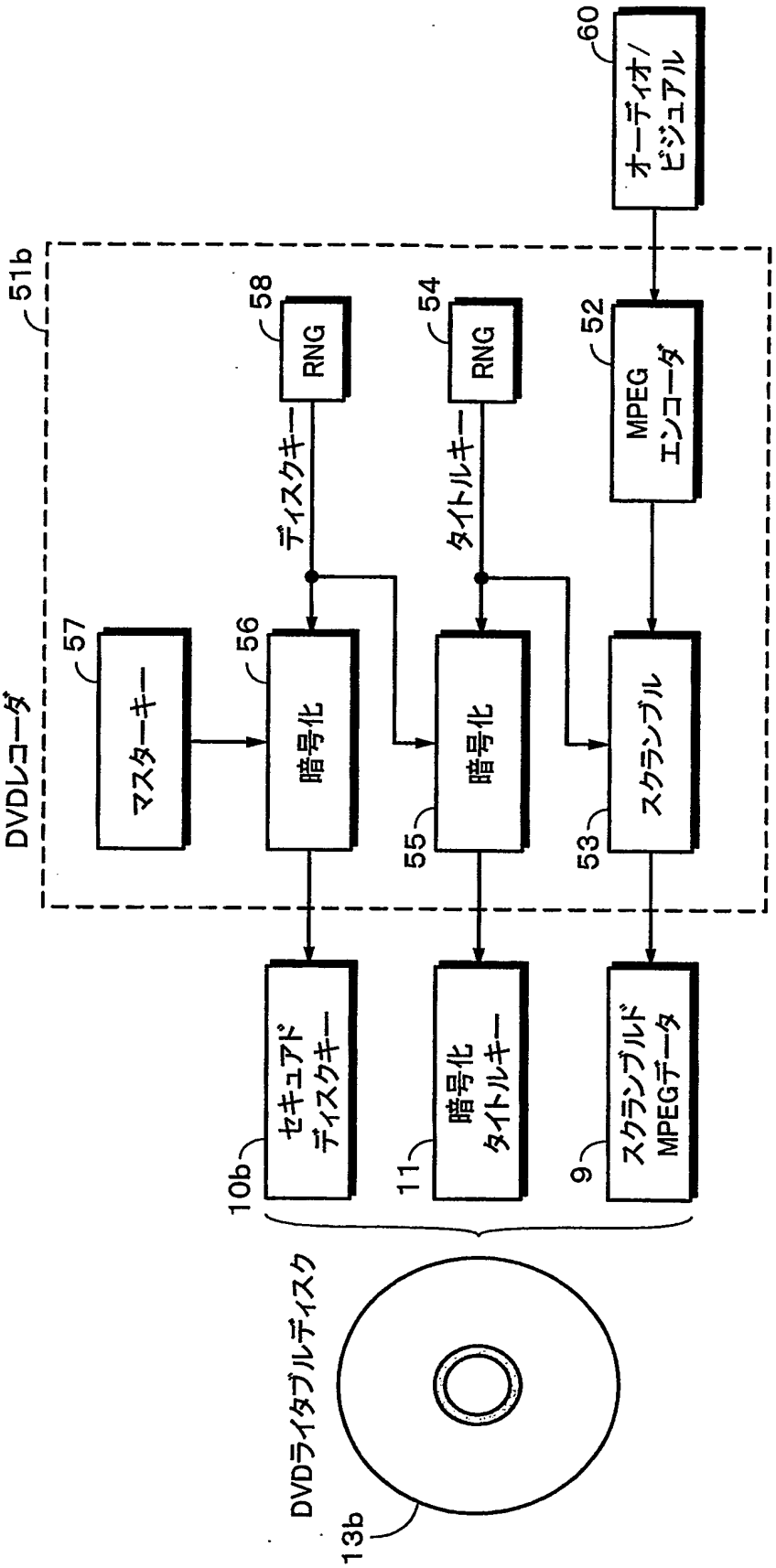
第7図


CSSスクランブルド
DVDメディア 12
DVDドライブ 31
PC 41
(ホスト)
AKE
S1
S2
コンテントデータゾーンを
シークおよびリード
S3
セキュアドディスクキーを要求
S4
セキュアドディスクキーをリード
S5
セキュアドディスク・キー
S6
Ksで暗号化されたセキュアドディスクキー
をリターン
S7
暗号化タイトルキー、CGMSを要求
S8
暗号化タイトルキー、CGMSをリード
S9
暗号化タイトルキー、CGMS
S10
暗号化タイトルキー、CGMSをリターン
S11
スクランブルドコンテンツを要求
S12
スクランブルドコンテンツをリード
S13
スクランブルドコンテンツ
S14
スクランブルドコンテンツをリターン

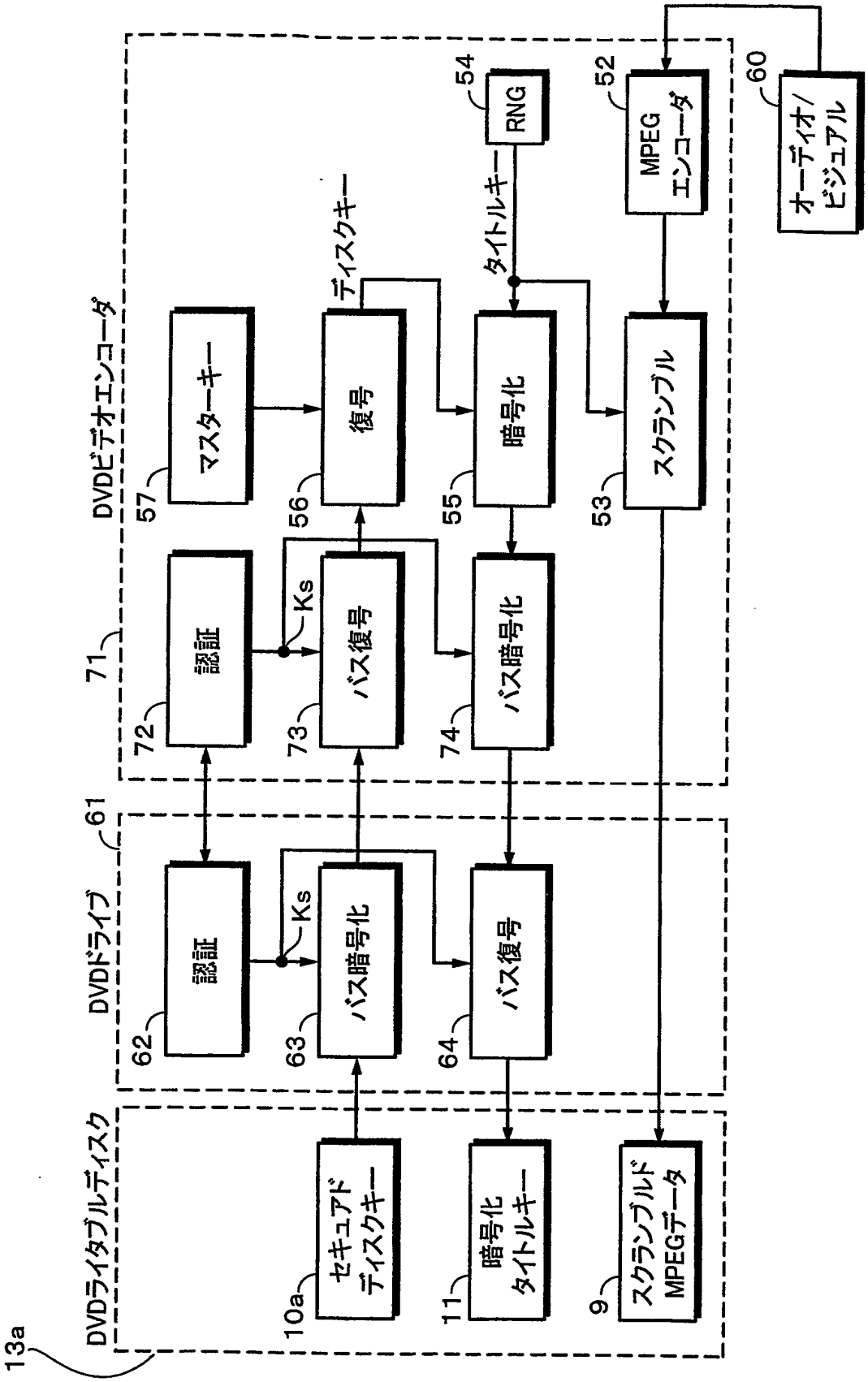
第８図


DVDレコーダ
51a
マスターキー
57
復号
56
ディスクキー
暗号化
55
タイトルキー
RNG
54
スクランブル
53
MPEG
エンコーダ
52
オーディオ/
ビジュアル
60
セキュアド
ディスクキー
10a
暗号化
タイトルキー
11
スクランブルド
MPEGデータ
9
DVDライタブルディスク
13a

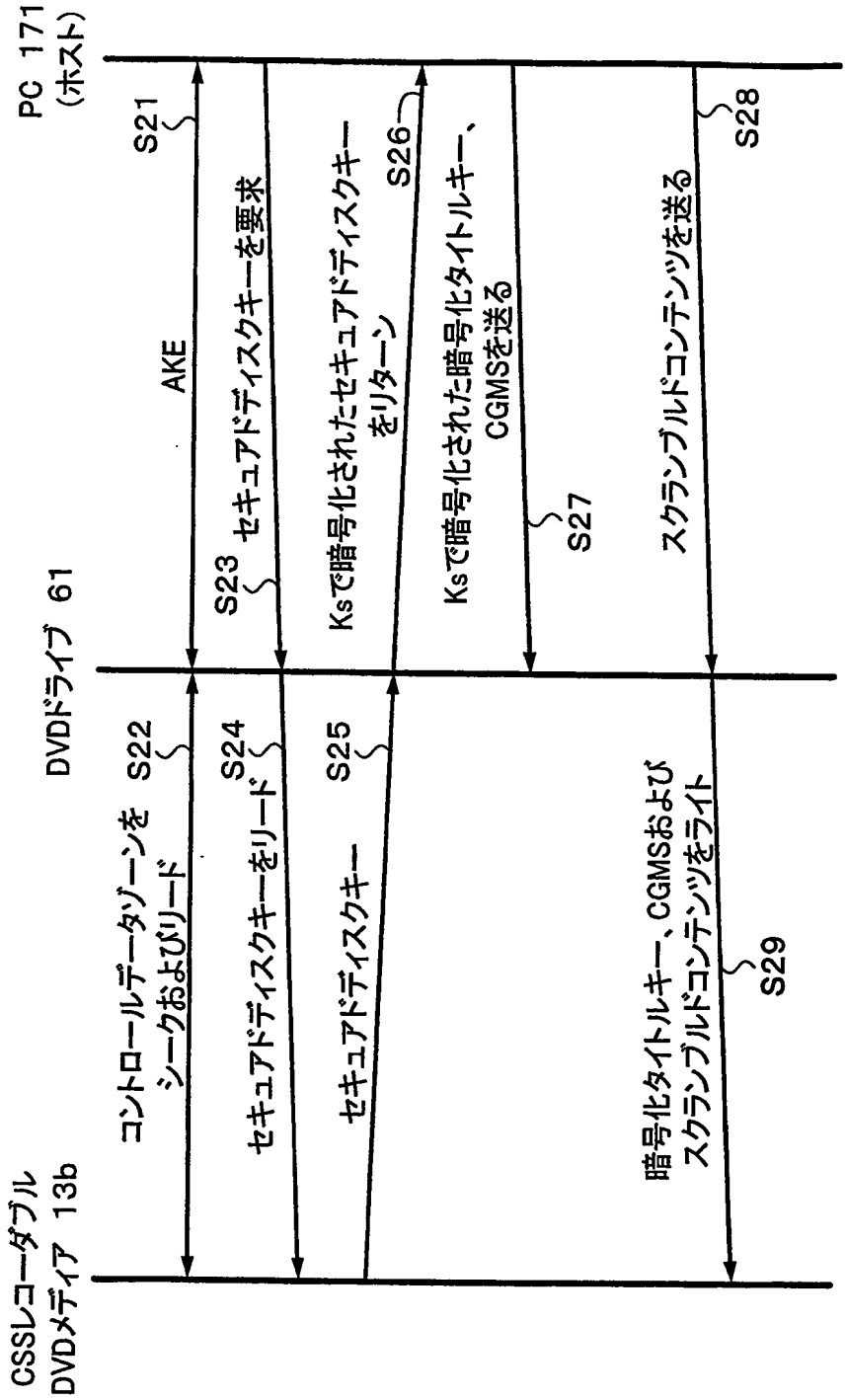
第9図


DVDレコーダ
51b
マスターキー
57
暗号化
56
RNG
58
ディスクキー
暗号化
55
RNG
54
タイトルキー
スクランブル
53
MPEG
エンコーダ
52
オーディオ/
ビジュアル
60
セキュアド
ディスクキー
10b
暗号化
タイトルキー
11
スクランブルド
MPEGデータ
9
DVDライタブルディスク
13b

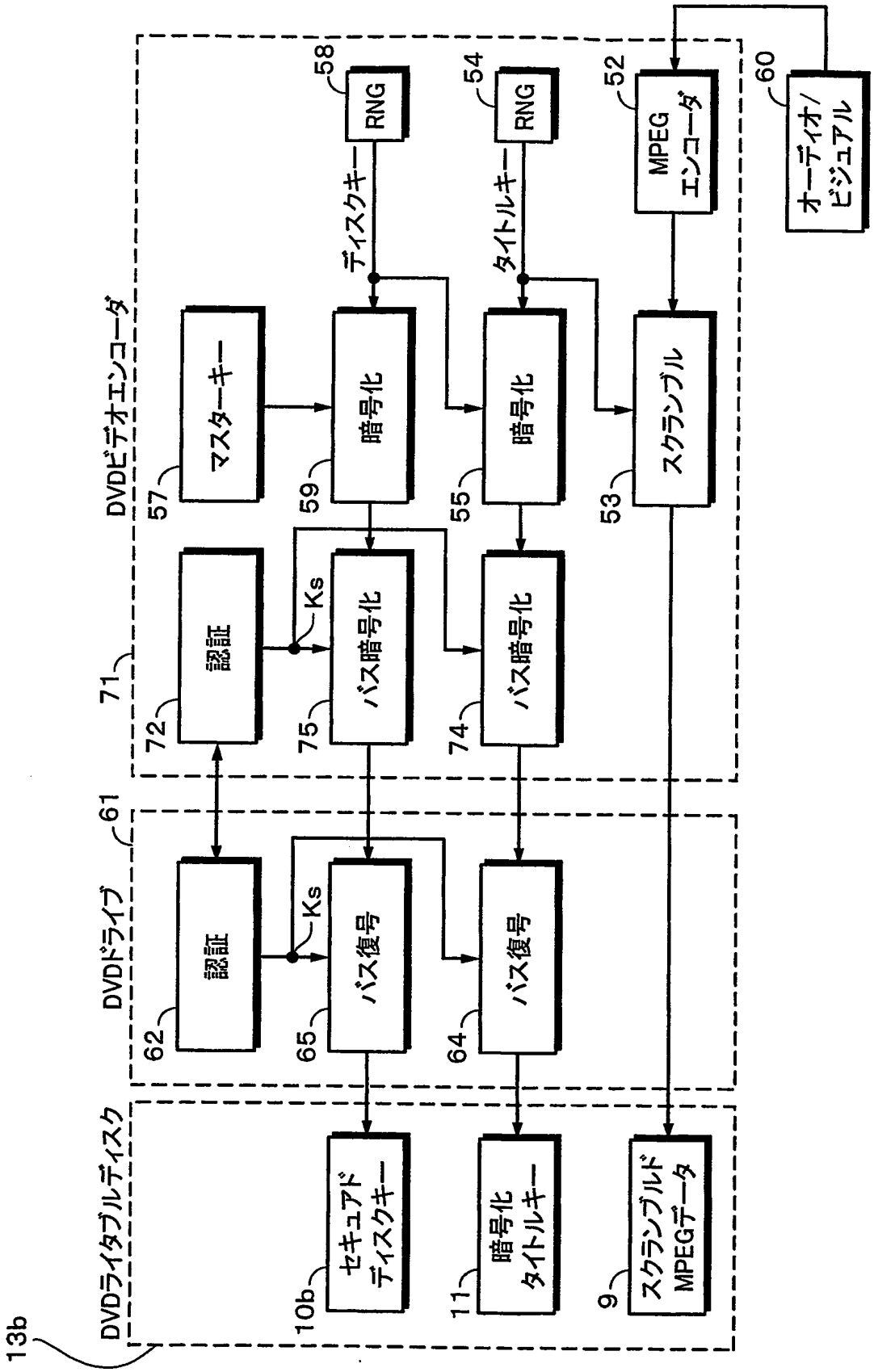
第１０図


13a
DVDライタブルディスク
10a
セキュアド
ディスクキー
11
暗号化
タイトルキー
9
スクランブルド
MPEGデータ
DVDドライブ
61
62
認証
Ks
63
バス暗号化
64
バス復号
DVDビデオエンコーダ
71
72
認証
Ks
73
バス復号
74
バス暗号化
57
マスターキー
56
復号
ディスクキー
55
暗号化
タイトルキー
54
RNG
53
スクランブル
52
MPEG
エンコーダ
60
オーディオ/
ビジュアル

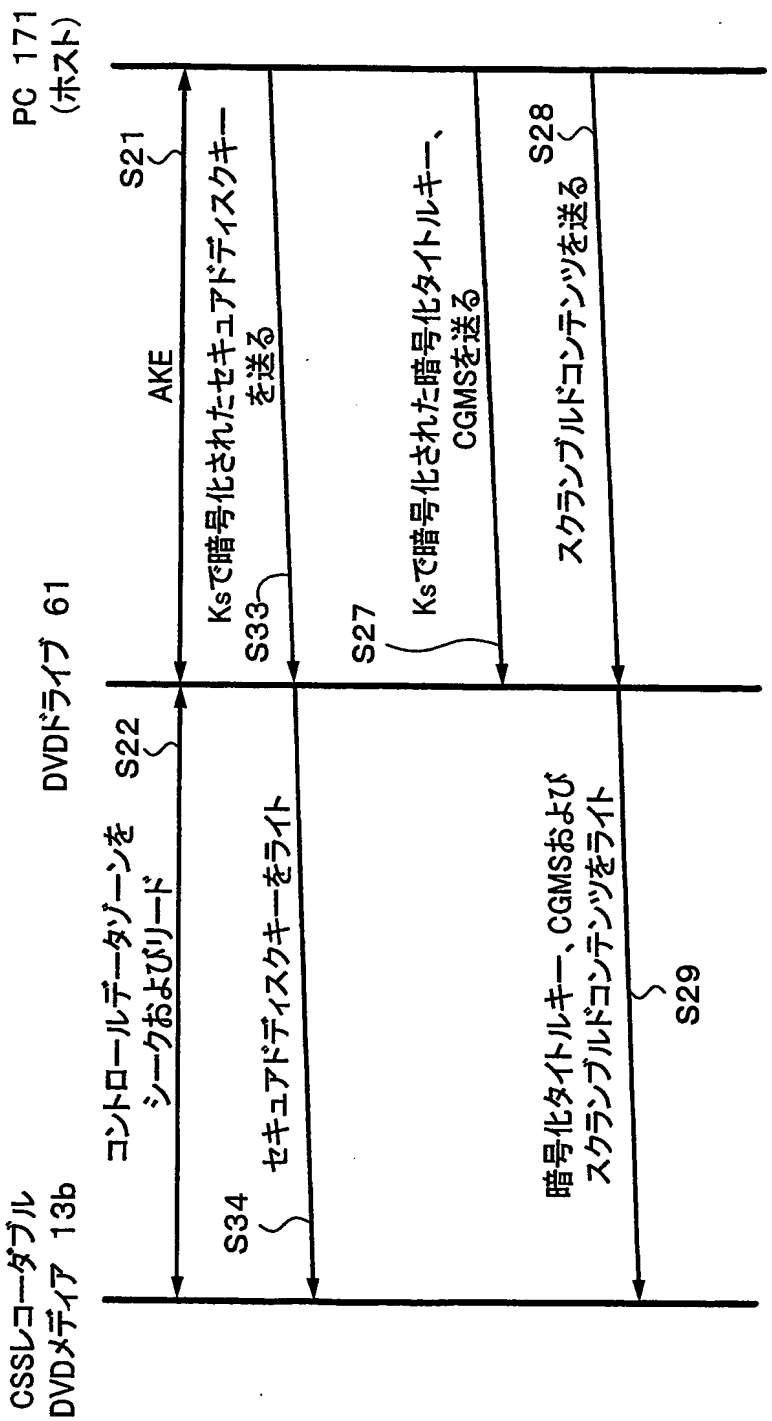
第１１図


PC 171
(ホスト)
DVDドライブ 61
CSSレコーダブル
DVDメディア 13b
AKE
S21
S22
コントロールデータゾーンを
シークおよびリード
S23
セキュアドディスクキーを要求
S24
セキュアドディスクキーをリード
S25
セキュアドディスクキー
S26
Ksで暗号化されたセキュアドディスクキー
をリターン
Ksで暗号化された暗号化タイトルキー、
CGMSを送る
S27
スクランブルドコンテンツを送る
S28
暗号化タイトルキー、CGMSおよび
スクランブルドコンテンツをライト
S29

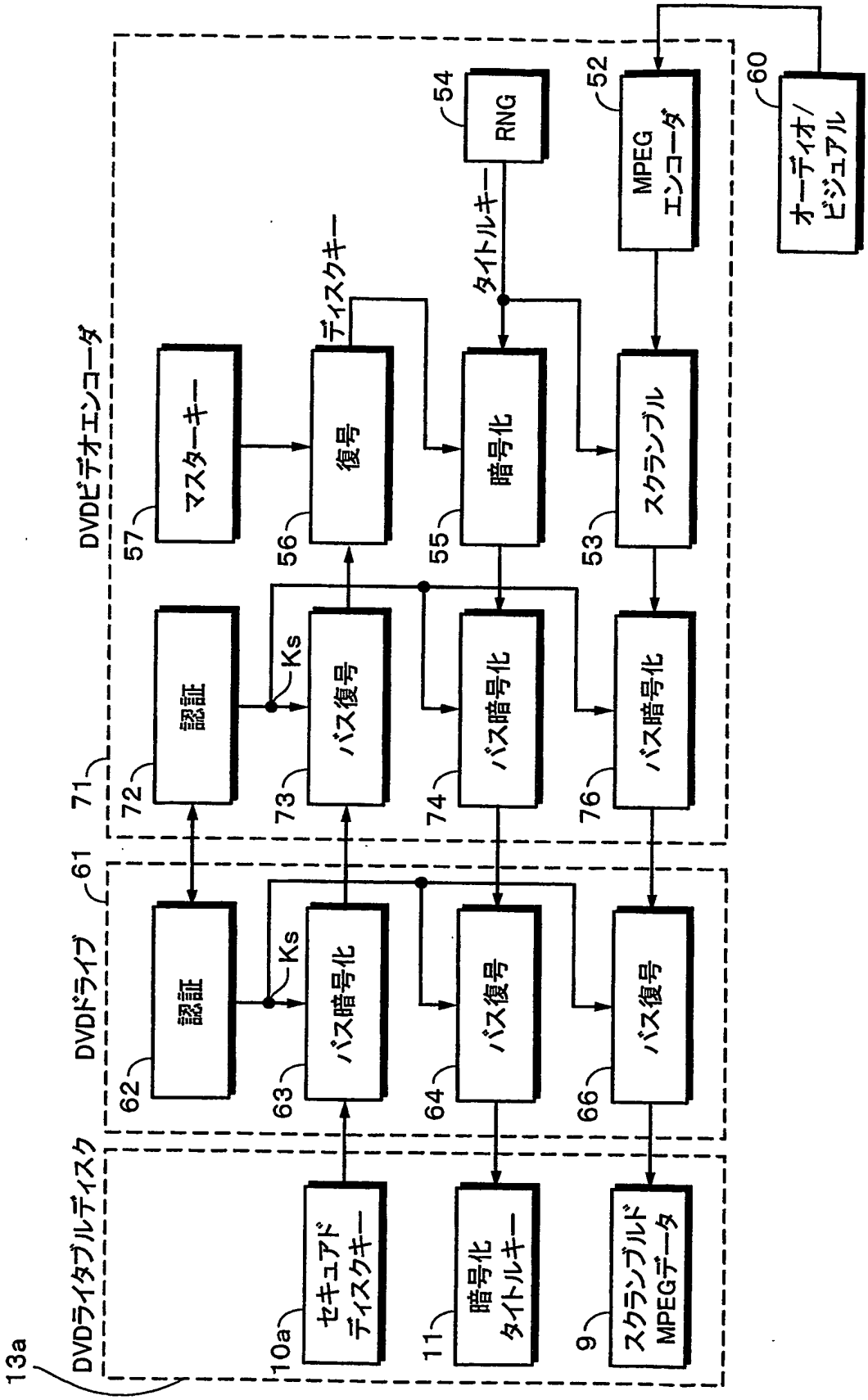
第１２図


13b
DVDライタブルディスク
DVDドライブ
61
DVDビデオエンコーダ
71
セキュアド
ディスクキー
10b
暗号化
タイトルキー
11
スクランブルド
MPEGデータ
9
認証
62
Ks
パス復号
65
パス復号
64
認証
72
Ks
パス暗号化
75
パス暗号化
74
マスターキー
57
暗号化
59
暗号化
55
スクランブル
53
RNG
58
RNG
54
MPEG
エンコーダ
52
オーディオ/
ビジュアル
60
ディスクキー
タイトルキー

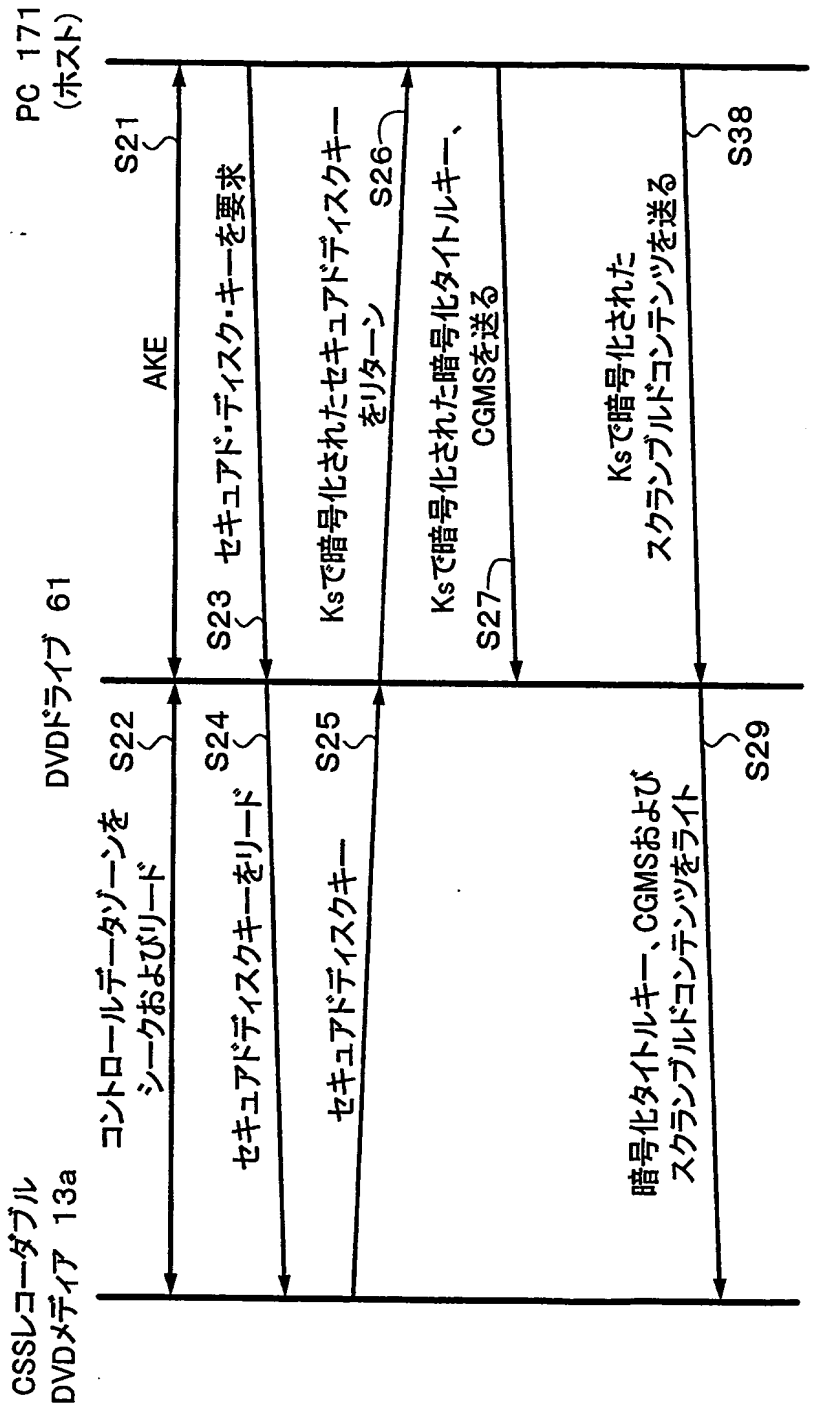
第１３図


PC 171
(ホスト)
DVDドライブ 61
CSSレコーダブル
DVDメディア 13b
AKE
S21
Ksで暗号化されたセキュアドディスクキー
を送る
S33
S27
Ksで暗号化された暗号化タイトルキー、
CGMSを送る
S28
スクランブルドコンテンツを送る
コントロールデータゾーンを
シークおよびリード
S22
セキュアドディスクキーをライト
S34
暗号化タイトルキー、CGMSおよび
スクランブルドコンテンツをライト
S29

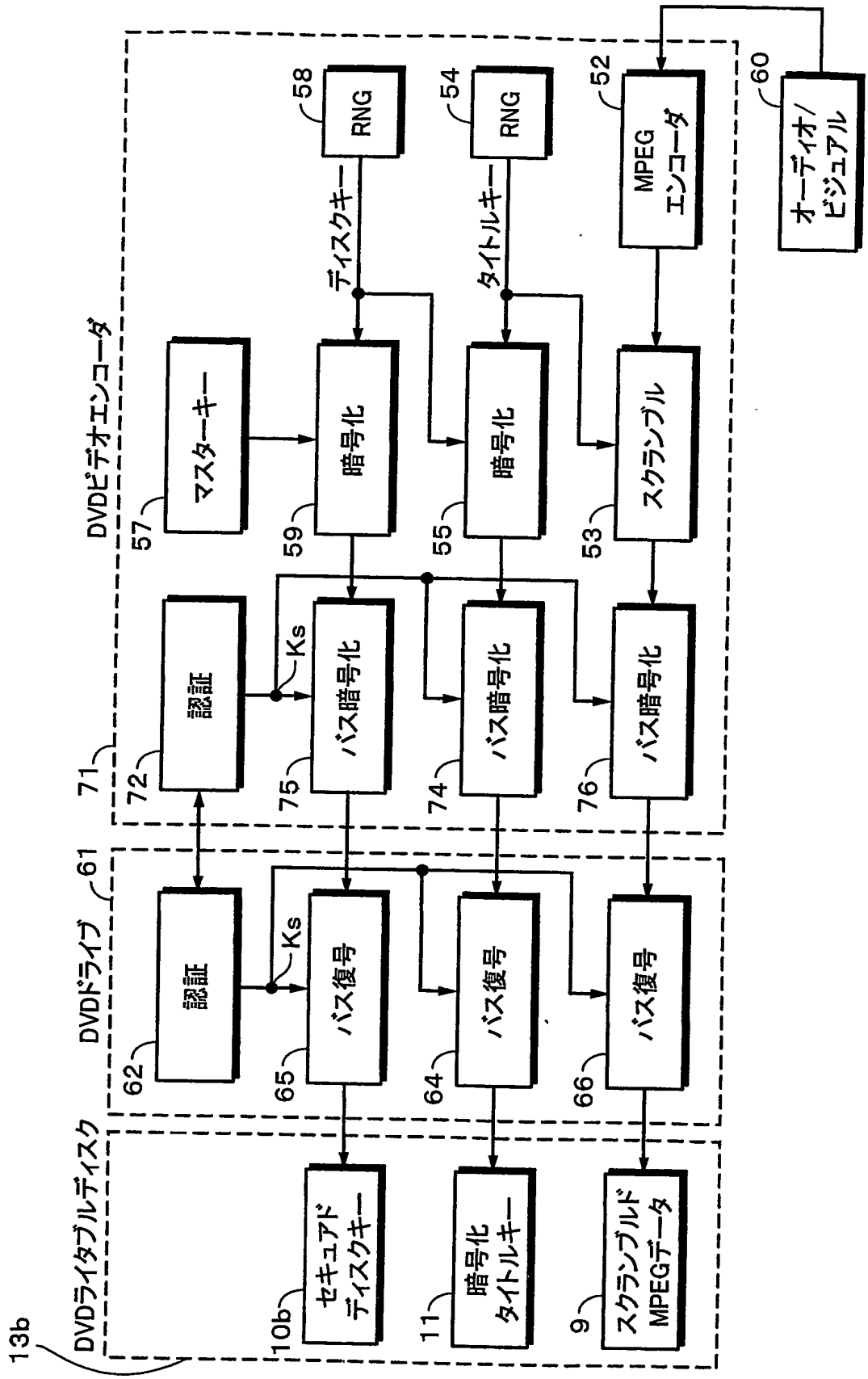
第１４図


13a
DVDライタブルディスク
DVDドライブ
61
DVDビデオエンコーダ
71
10a
セキュアド
ディスクキー
11
暗号化
タイトルキー
9
スクランブルド
MPEGデータ
62
認証
63
パス暗号化
64
パス復号
66
パス復号
72
認証
Ks
73
パス復号
74
パス暗号化
76
パス暗号化
57
マスターキー
56
復号
ディスクキー
55
暗号化
タイトルキー
54
RNG
53
スクランブル
52
MPEG
エンコーダ
60
オーディオ/
ビジュアル

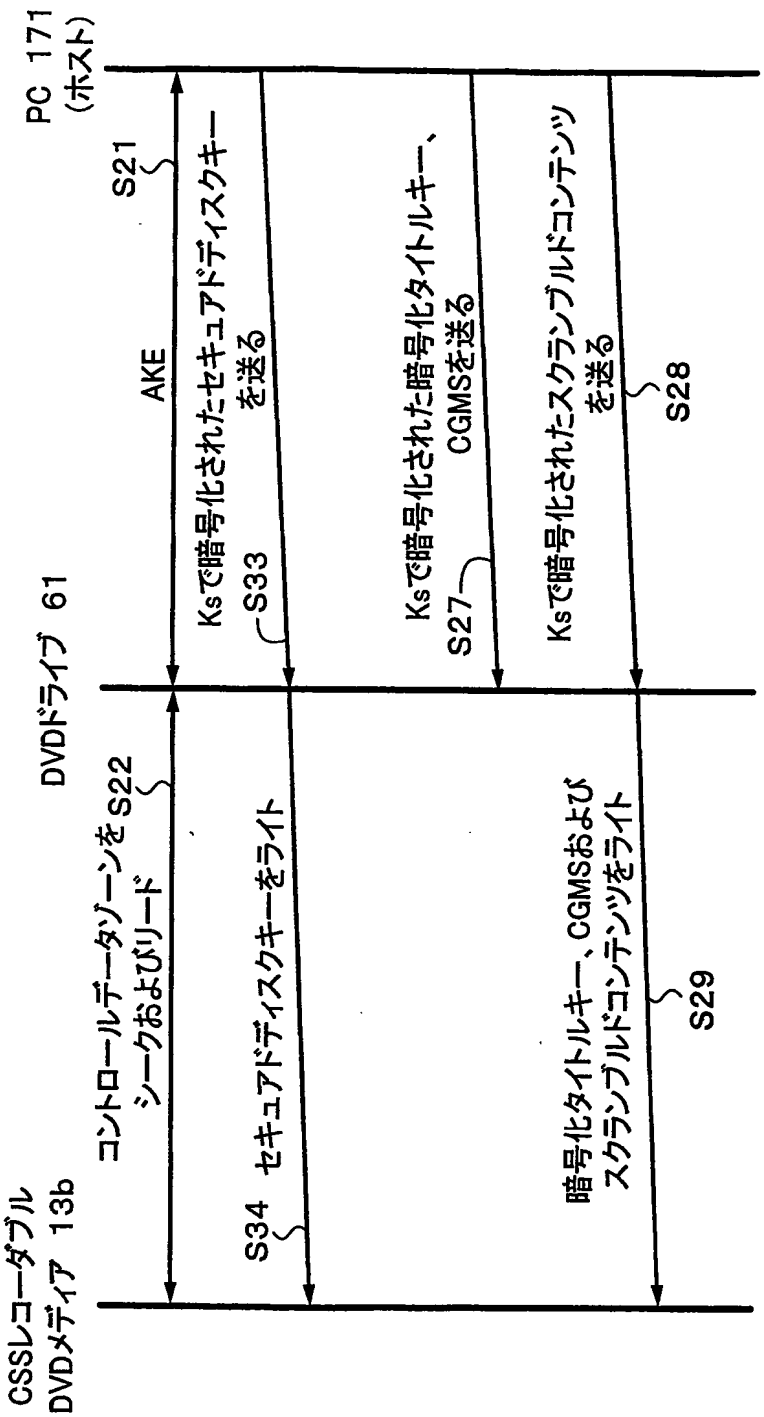
第15図


PC 171
(ホスト)
DVDドライブ 61
CSSレコーダブル
DVDメディア 13a
AKE
S21
S22
コントロールデータゾーンを
シークおよびリード
S23
セキュアド・ディスク・キーを要求
S24
セキュアドディスクキーをリード
S25
セキュアドディスクキー
S26
Ksで暗号化されたセキュアドディスクキー
をリターン
S27
Ksで暗号化された暗号化タイトルキー、
CGMSを送る
S29
暗号化タイトルキー、CGMSおよび
スクランブルドコンテンツをライト
S38
Ksで暗号化された
スクランブルドコンテンツを送る

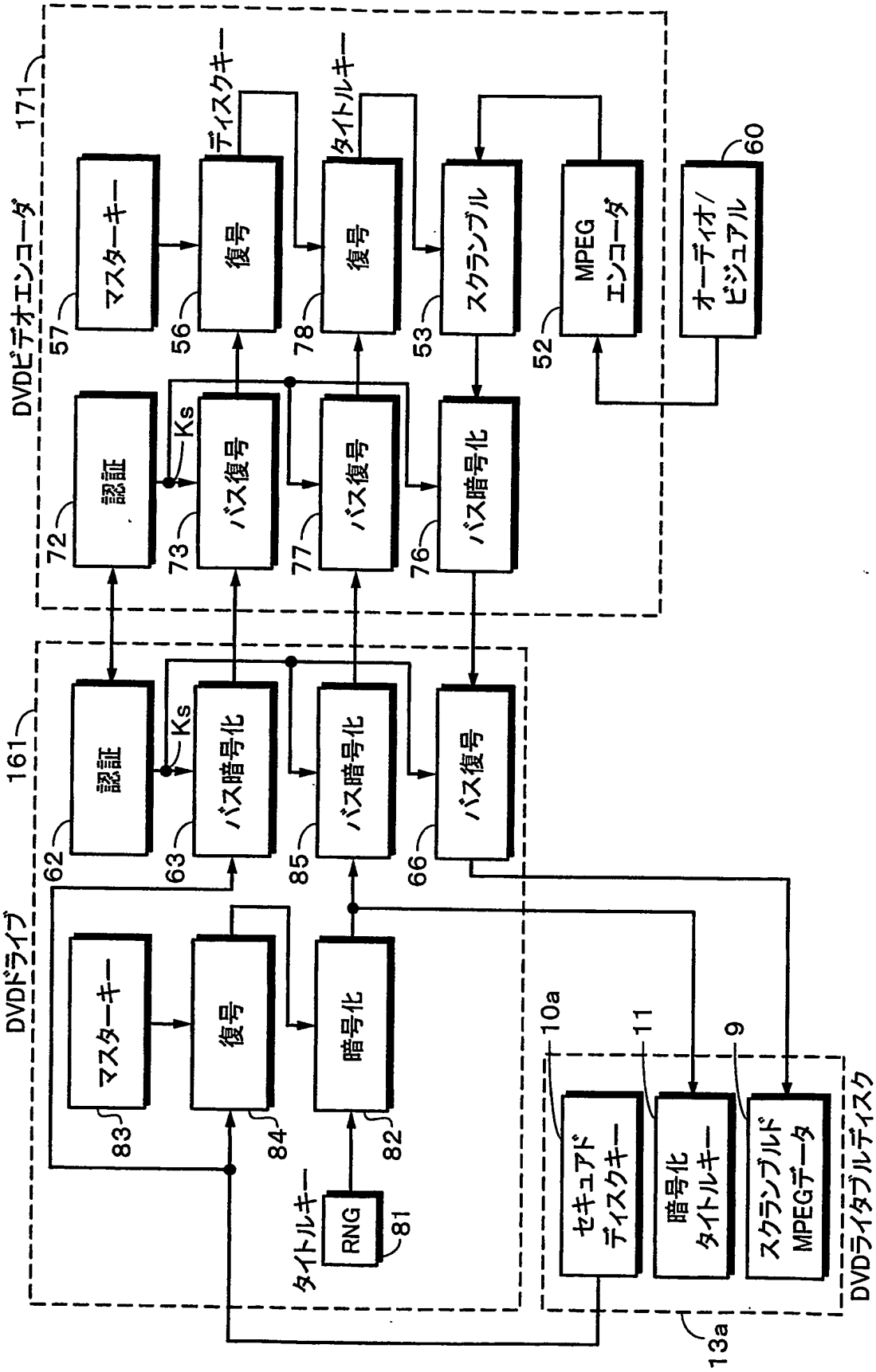
第１６図


13b
DVDライタブルディスク
DVDドライブ
61
DVDビデオエンコーダ
71
認証
62
認証
72
Ks
Ks
バス復号
65
バス復号
64
バス復号
66
バス暗号化
75
バス暗号化
74
バス暗号化
76
セキュアド
ディスクキー
10b
暗号化
タイトルキー
11
スクランブルド
MPEGデータ
9
マスターキー
57
暗号化
59
暗号化
55
スクランブル
53
RNG
58
RNG
54
MPEG
エンコーダ
52
オーディオ/
ビジュアル
60
ディスクキー
タイトルキー

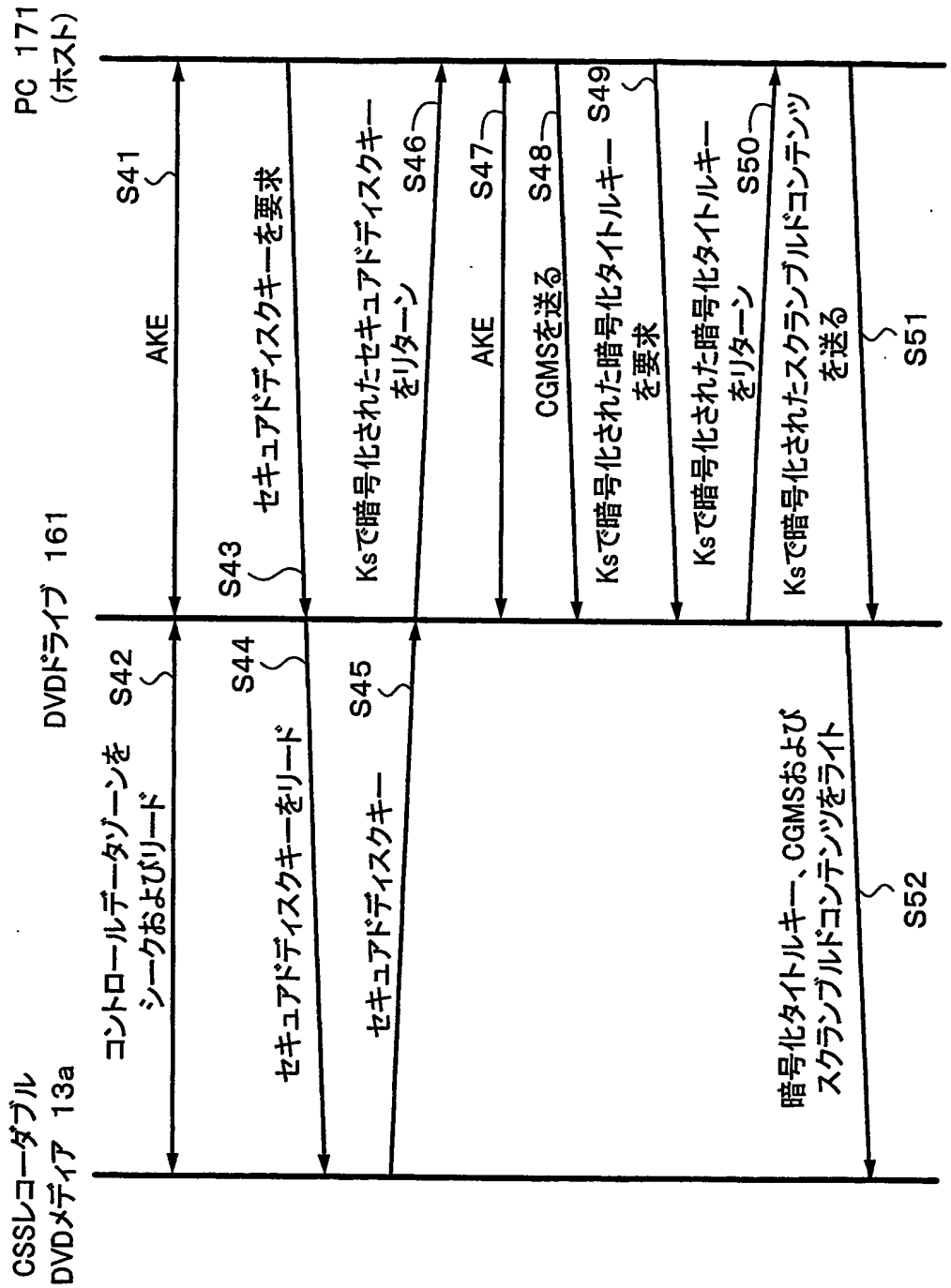
第１７図


PC 171
(ホスト)
DVDドライブ 61
CSSレコーダブル
DVDメディア 13b
AKE
S21
Ksで暗号化されたセキュアドディスクキー
を送る
S33
コントロールデータゾーンを
シークおよびリード
S22
セキュアドディスクキーをライト
S34
Ksで暗号化された暗号化タイトルキー、
CGMSを送る
S27
Ksで暗号化されたスクランブルドコンテンツ
を送る
S28
暗号化タイトルキー、CGMSおよび
スクランブルドコンテンツをライト
S29

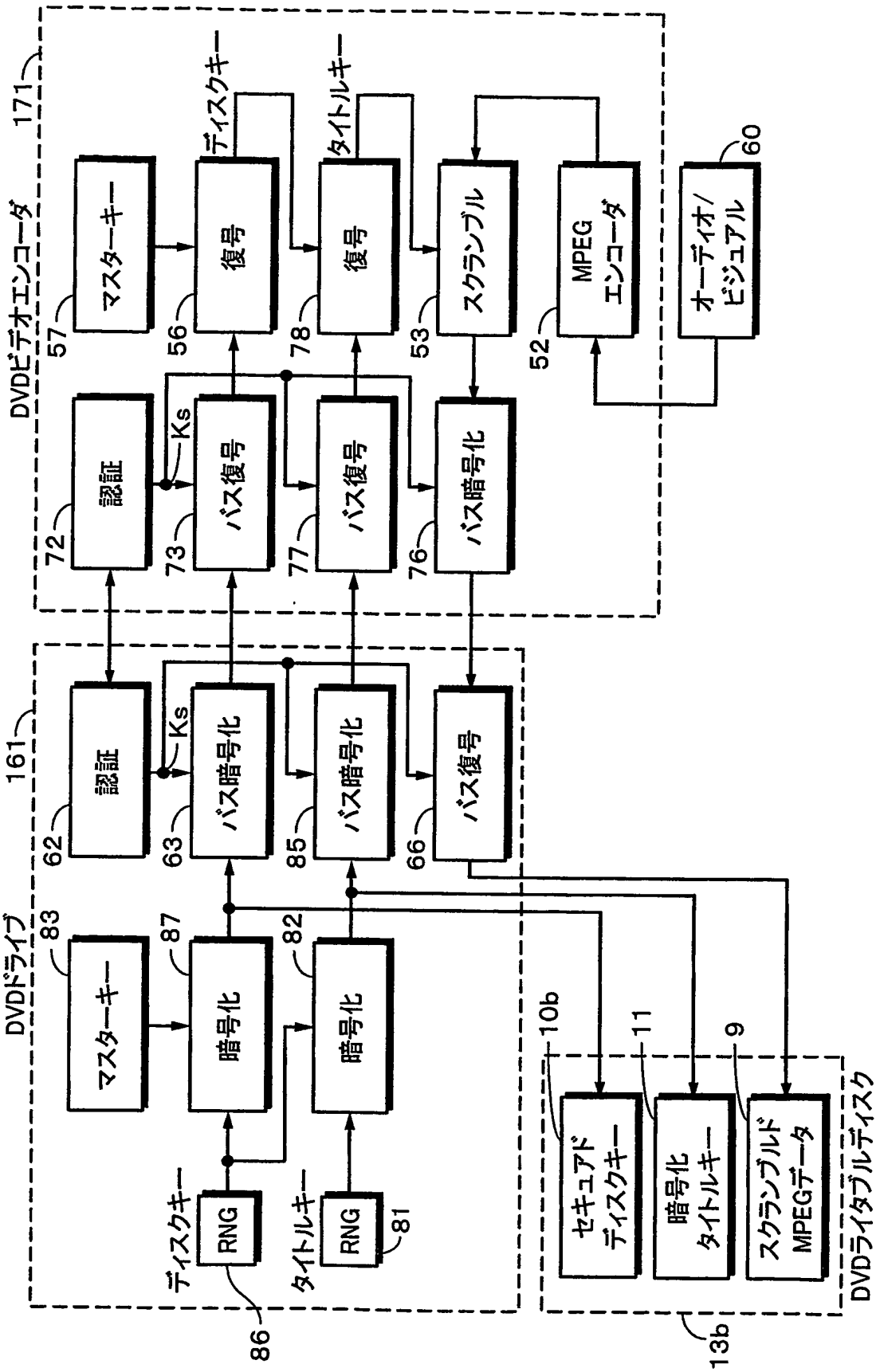
第１８図


DVDビデオエンコーダ
171
マスターキー
57
復号
56
ディスクキー
復号
78
タイトルキー
スクランブル
53
MPEG
エンコーダ
52
オーディオ/
ビジュアル
60
認証
72
Ks
バス復号
73
バス復号
77
バス暗号化
76
161
認証
62
Ks
バス暗号化
63
バス暗号化
85
バス復号
66
DVDドライブ
マスターキー
83
復号
84
暗号化
82
タイトルキー
RNG
81
10a
11
9
セキュアド
ディスクキー
暗号化
タイトルキー
スクランブルド
MPEGデータ
DVDライタブルディスク
13a

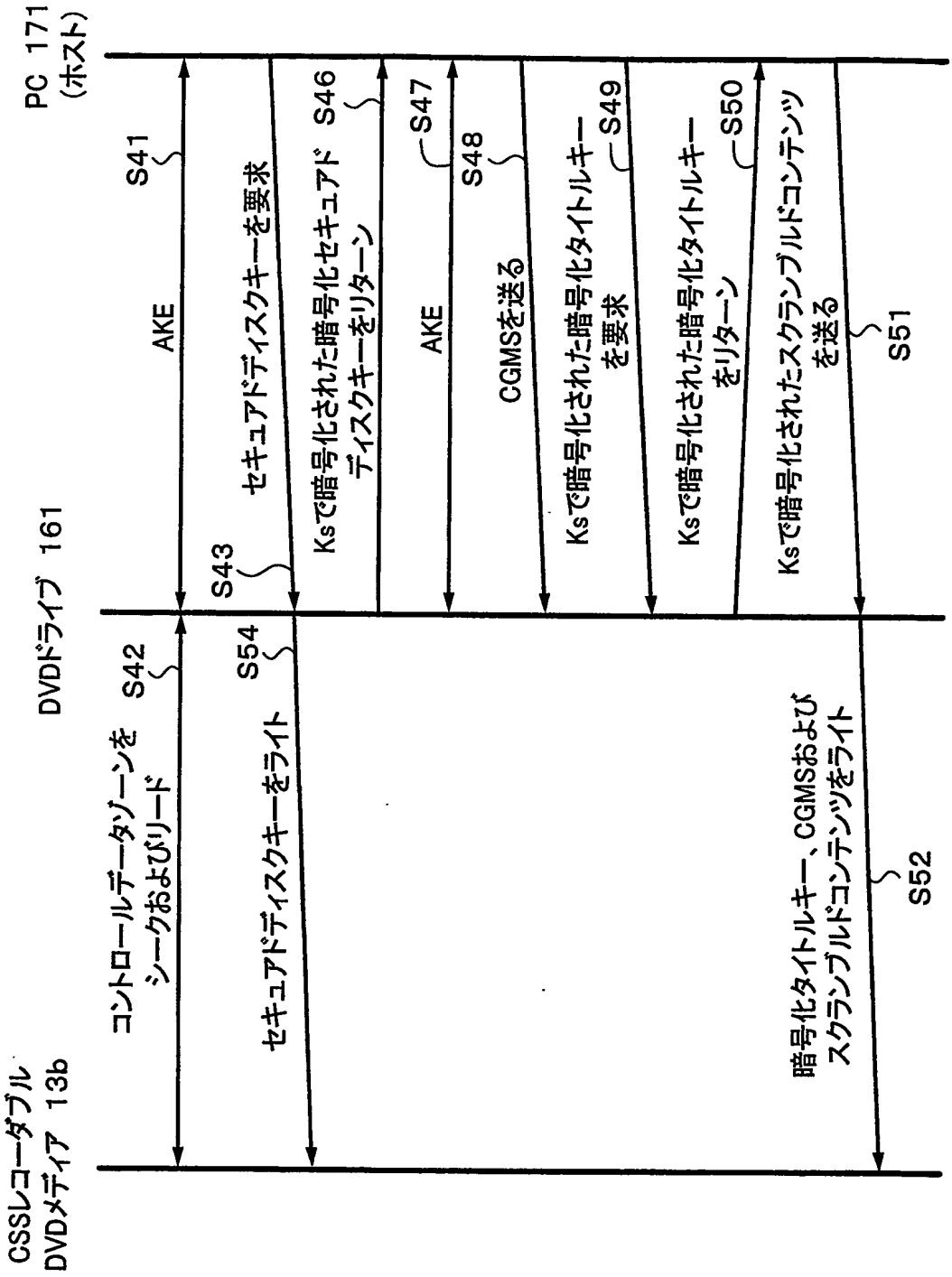
第19図


PC 171
(ホスト)
DVDドライブ 161
CSSレコーダブル
DVDメディア 13a
AKE
S41
セキュアドディスクキーを要求
S43
Ksで暗号化されたセキュアドディスクキー
をリターン
S46
AKE
S47
CGMSを送る
S48
Ksで暗号化された暗号化タイトルキー
を要求
S49
Ksで暗号化された暗号化タイトルキー
をリターン
S50
Ksで暗号化されたスクランブルドコンテンツ
を送る
S51
コントロールデータゾーンを
シークおよびリード
S42
セキュアドディスクキーをリード
S44
セキュアドディスクキー
S45
暗号化タイトルキー、CGMSおよび
スクランブルドコンテンツをライト
S52

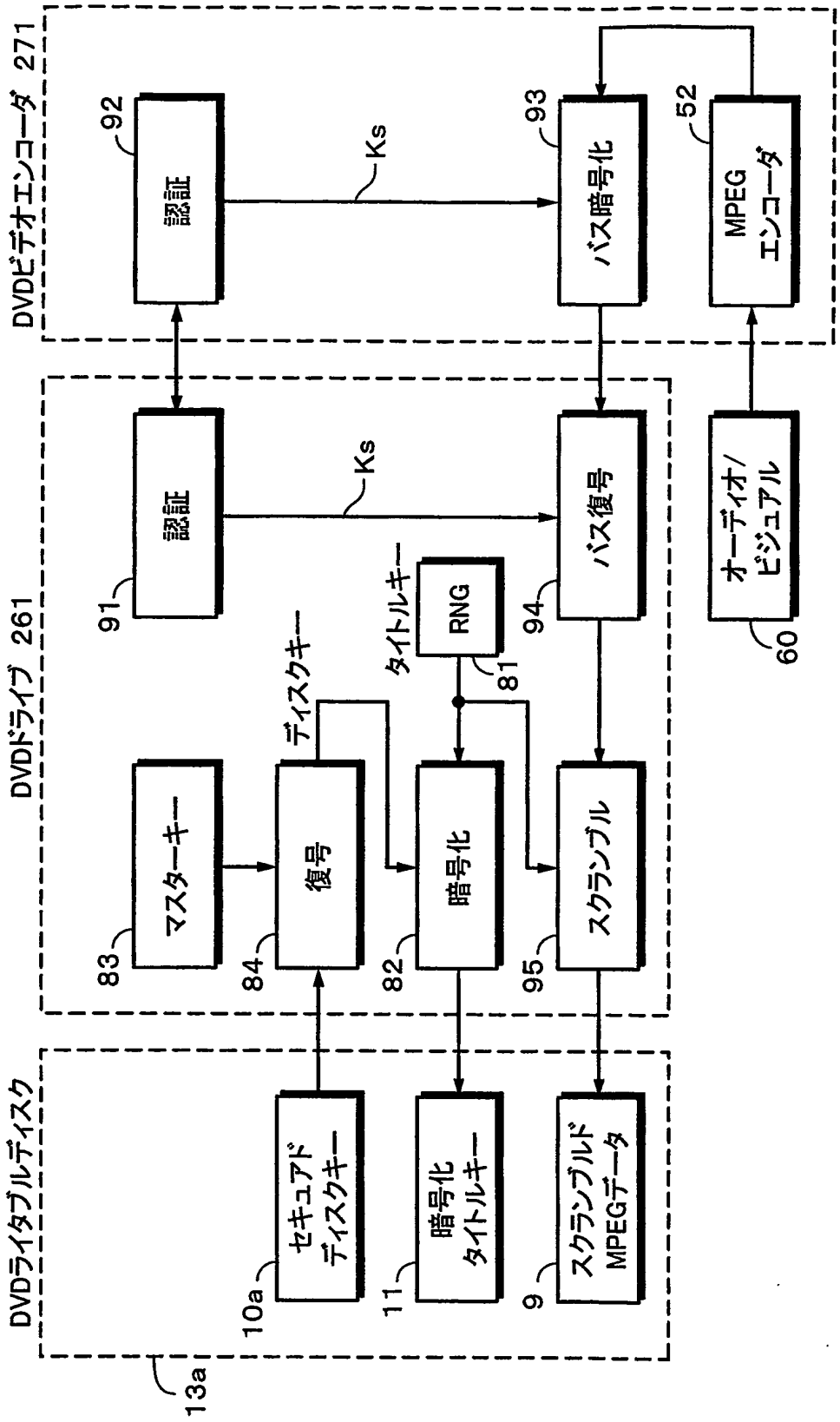
第２０図


DVDビデオエンコーダ
171
マスターキー
57
ディスクキー
復号
56
タイトルキー
復号
78
スクランブル
53
MPEG
エンコーダ
52
オーディオ/
ビジュアル
60
認証
72
Ks
パス復号
73
パス復号
77
パス暗号化
76
161
認証
62
Ks
パス暗号化
63
パス暗号化
85
パス復号
66
DVDドライブ
83
マスターキー
87
暗号化
82
暗号化
ディスクキー
RNG
タイトルキー
RNG
81
86
10b
11
9
セキュアド
ディスクキー
暗号化
タイトルキー
スクランブルド
MPEGデータ
DVDライタブルディスク
13b

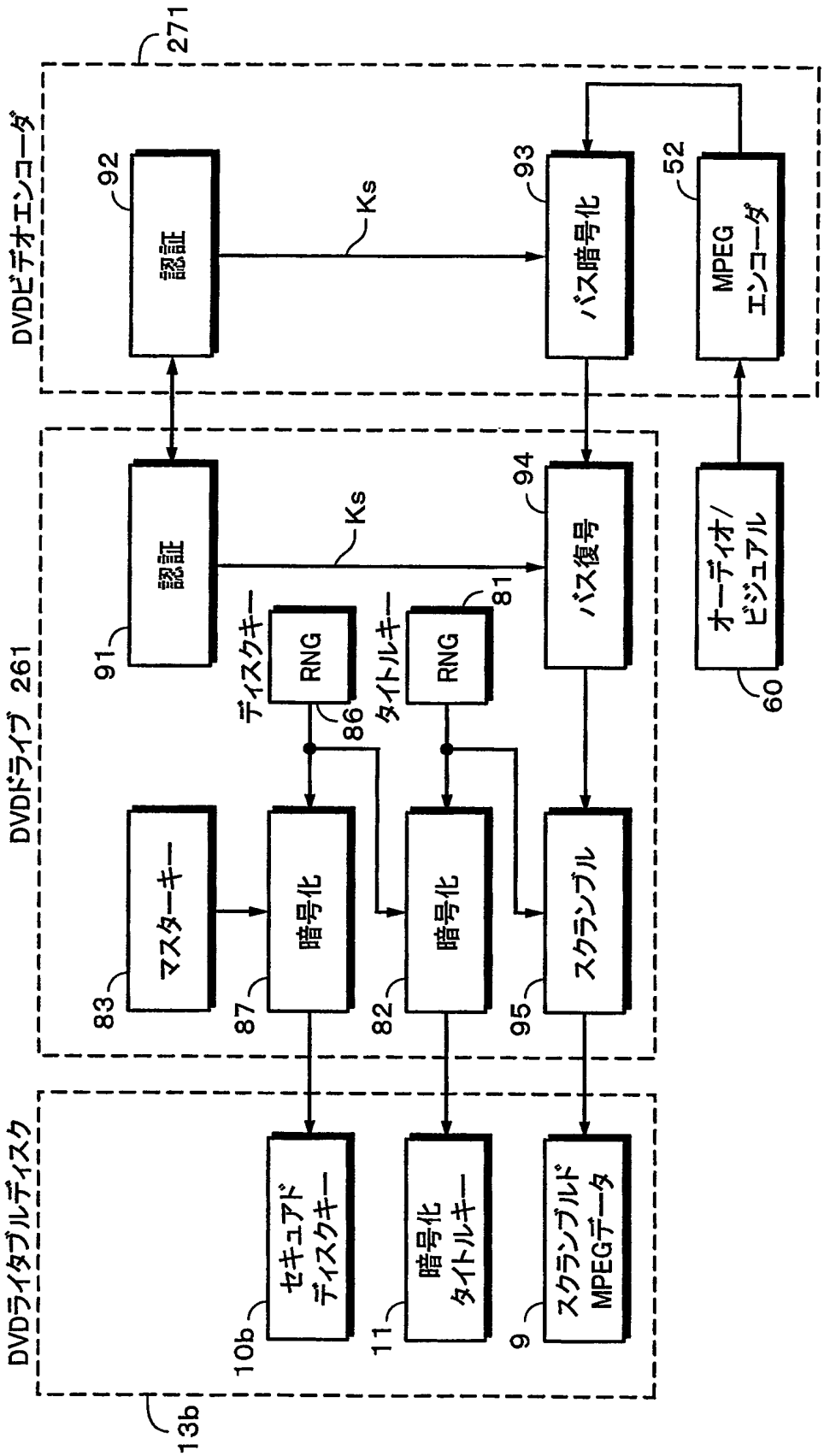
第２１図


PC 171
(ホスト)
DVDドライブ 161
CSSレコーダブル
DVDメディア 13b
S41
AKE
S43
セキュアドディスクキーを要求
S46
Ksで暗号化された暗号化セキュアド
ディスクキーをリターン
S47
AKE
S48
CGMSを送る
S49
Ksで暗号化された暗号化タイトルキー
を要求
S50
Ksで暗号化された暗号化タイトルキー
をリターン
S51
Ksで暗号化されたスクランブルドコンテンツ
を送る
S42
コントロールデータゾーンを
シークおよびリード
S54
セキュアドディスクキーをライト
S52
暗号化タイトルキー、CGMSおよび
スクランブルドコンテンツをライト

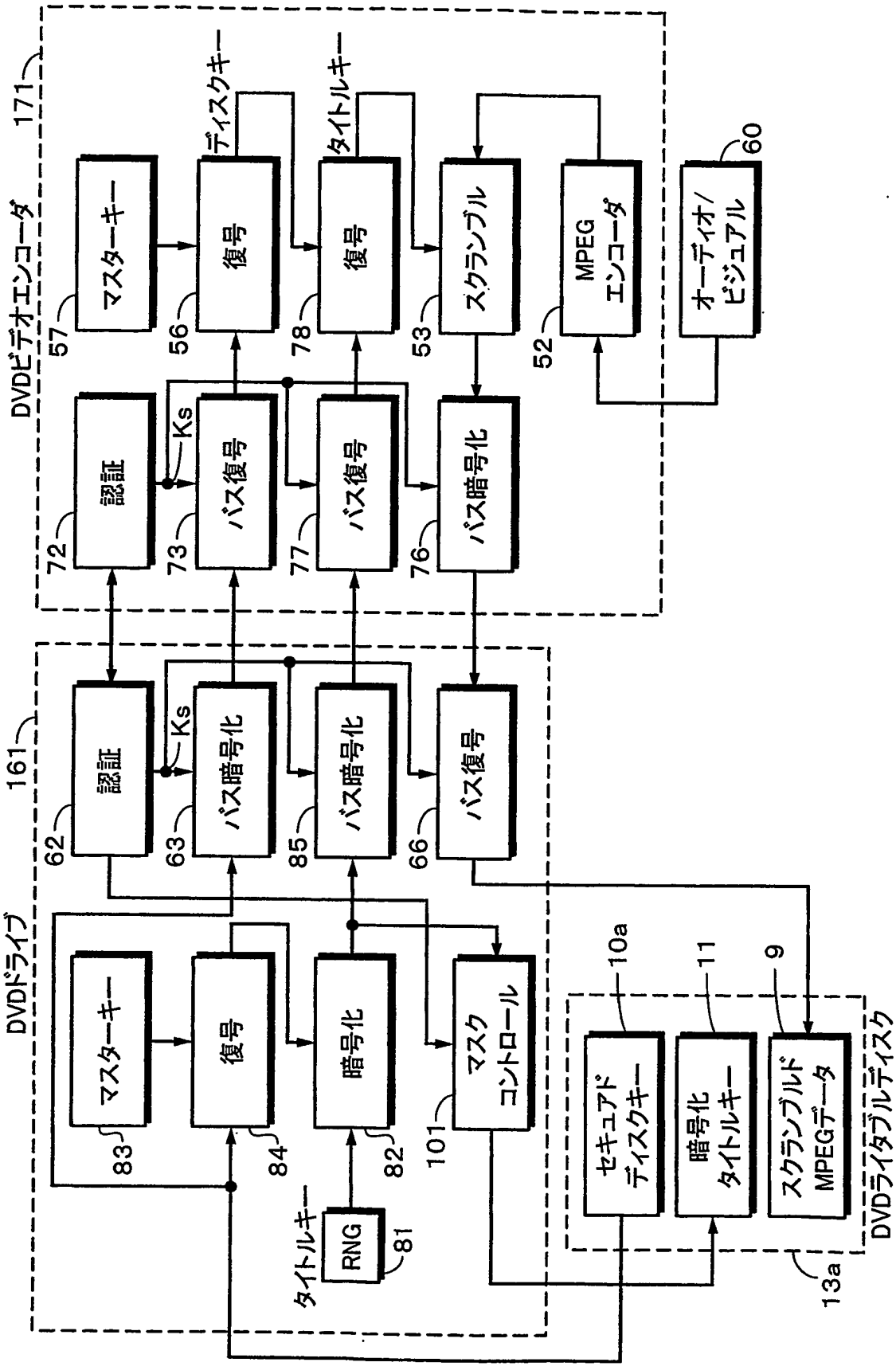
第２２図


DVDビデオエンコーダ 271
92
認証
Ks
93
バス暗号化
52
MPEG
エンコーダ
DVDドライブ 261
91
認証
Ks
94
バス復号
60
オーディオ/
ビジュアル
タイトルキー
RNG
81
ディスクキー
83
マスターキー
84
復号
82
暗号化
95
スクランブル
DVDライタブルディスク
10a
セキュアド
ディスクキー
11
暗号化
タイトルキー
9
スクランブルド
MPEGデータ
13a

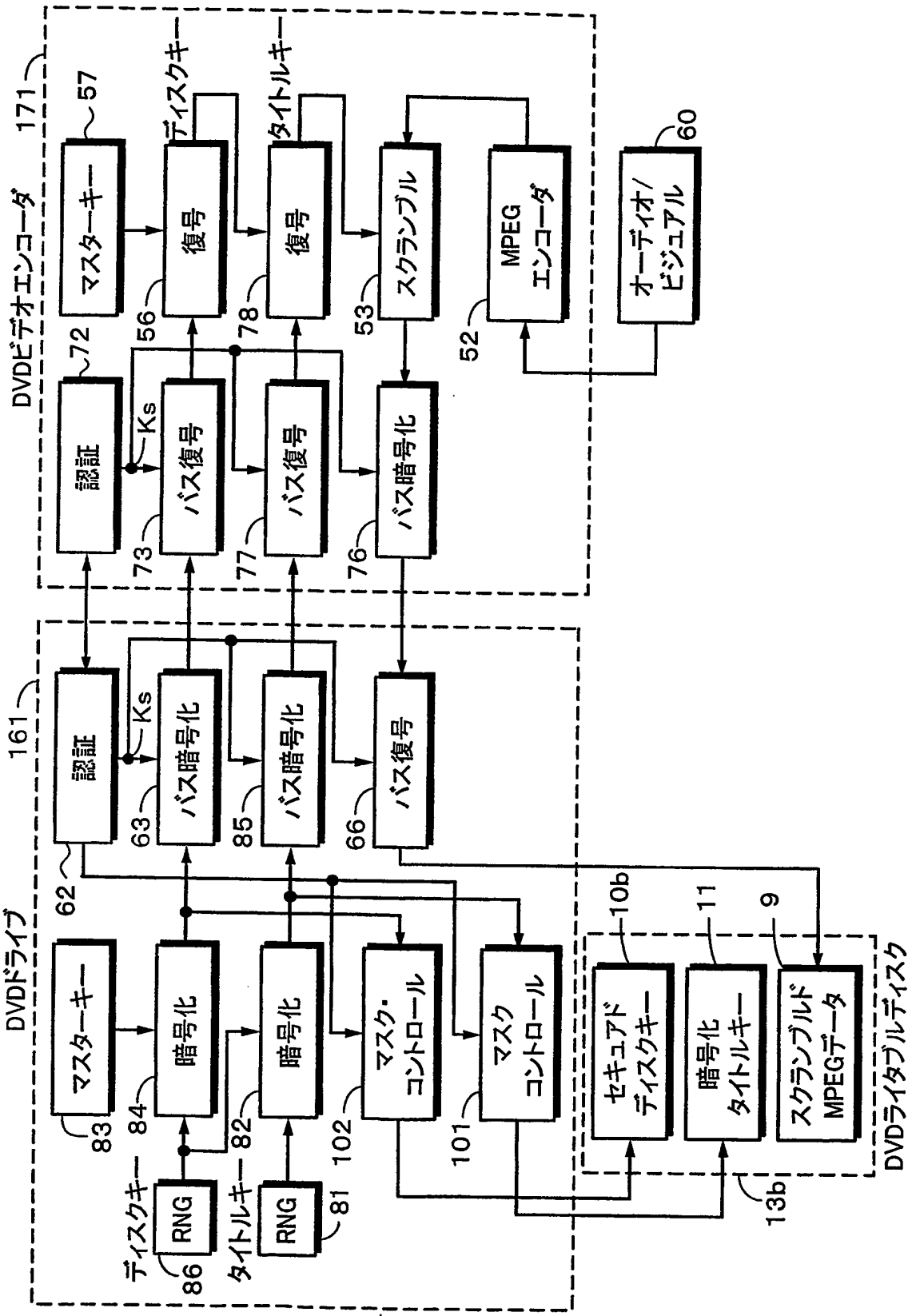
第２３図


DVDビデオエンコーダ
271
92
認証
Ks
93
バス暗号化
52
MPEG
エンコーダ
DVDドライブ 261
91
認証
Ks
94
バス復号
81
ディスクキー
RNG
86
タイトルキー
RNG
60
オーディオ/
ビジュアル
83
マスターキー
87
暗号化
82
暗号化
95
スクランブル
DVDライタブルディスク
10b
セキュアド
ディスクキー
11
暗号化
タイトルキー
9
スクランブルド
MPEGデータ
13b

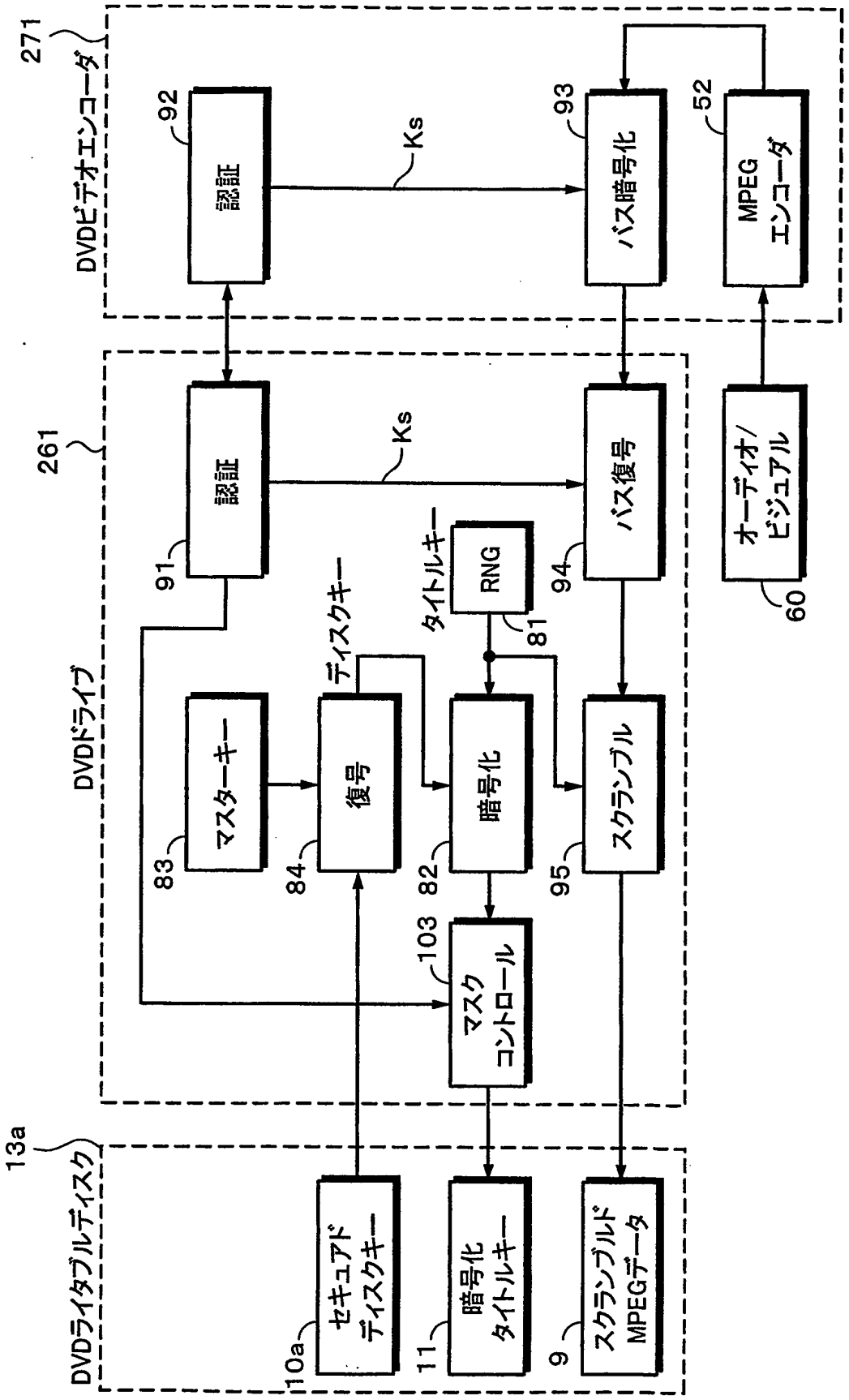
第２４図


DVDビデオエンコーダ
171
マスターキー
57
復号
56
ディスクキー
復号
78
タイトルキー
スクランブル
53
MPEG
エンコーダ
52
オーディオ/
ビジュアル
60
認証
72
Ks
パス復号
73
パス復号
77
パス暗号化
76
161
認証
62
Ks
パス暗号化
63
パス暗号化
85
パス復号
66
DVDドライブ
マスターキー
83
復号
84
暗号化
82
マスク
コントロール
101
タイトルキー
RNG
81
10a
11
9
セキュアド
ディスクキー
暗号化
タイトルキー
スクランブルド
MPEGデータ
DVDライタブルディスク
13a

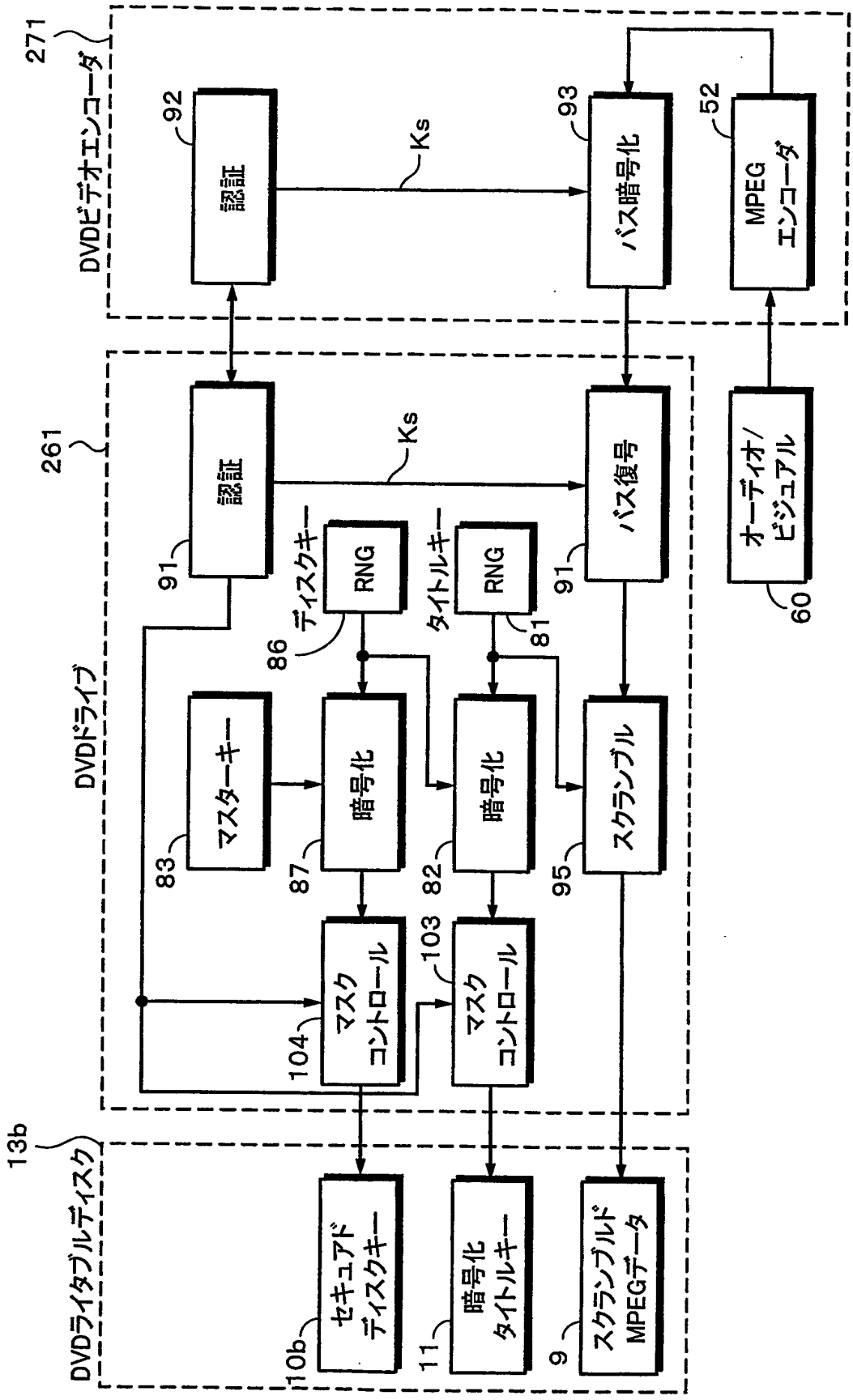
第25図


DVDビデオエンコーダ
171
マスターキー
57
ディスクキー
タイトルキー
復号
56
78
スクランブル
53
MPEG
エンコーダ
52
オーディオ/
ビジュアル
60
認証
72
Ks
パス復号
73
77
パス暗号化
76
161
パス暗号化
63
85
パス復号
66
62
DVDドライブ
マスターキー
83
暗号化
84
82
マスク・
コントロール
102
マスク
コントロール
101
10b
11
9
セキュアド
ディスクキー
暗号化
タイトルキー
スクランブルド
MPEGデータ
DVDライタブルディスク
13b
ディスクキー
RNG
86
タイトルキー
RNG
81

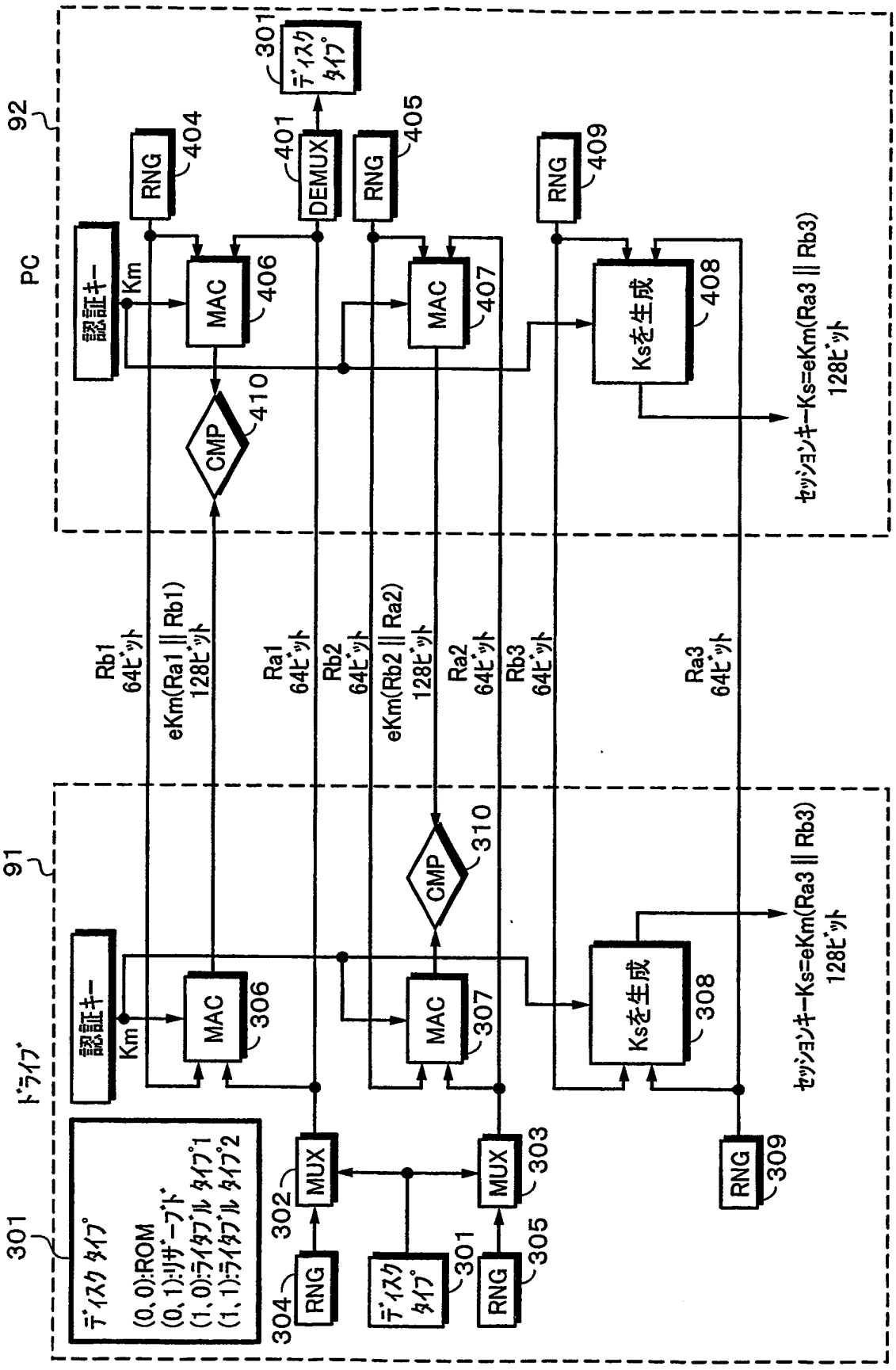
第２６図


271
DVDビデオエンコーダ
92
認証
Ks
93
バス暗号化
52
MPEG
エンコーダ
261
DVDドライブ
91
認証
Ks
94
バス復号
60
オーディオ/
ビジュアル
タイトルキー
RNG
81
ディスクキー
83
マスターキー
84
復号
82
暗号化
95
スクランブル
103
マスク
コントロール
13a
DVDライタブルディスク
10a
セキュアド
ディスクキー
11
暗号化
タイトルキー
9
スクランブルド
MPEGデータ

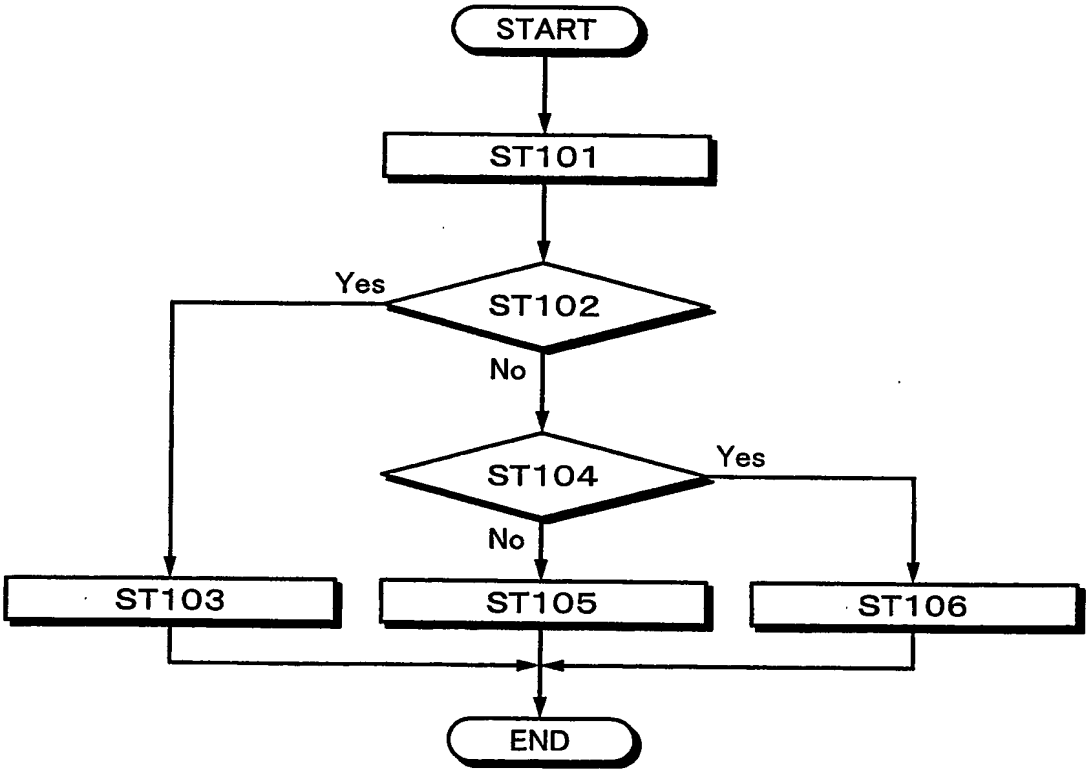
第27図


271
DVDビデオエンコーダ
92
認証
Ks
93
バス暗号化
52
MPEG
エンコーダ
261
DVDドライブ
91
認証
Ks
91
バス復号
60
オーディオ/
ビジュアル
ディスクキー
86
RNG
タイトルキー
81
RNG
83
マスターキー
87
暗号化
82
暗号化
95
スクランブル
104
マスク
コントロール
103
マスク
コントロール
13b
DVDライタブルディスク
10b
セキュアド
ディスクキー
11
暗号化
タイトルキー
9
スクランブルド
MPEGデータ

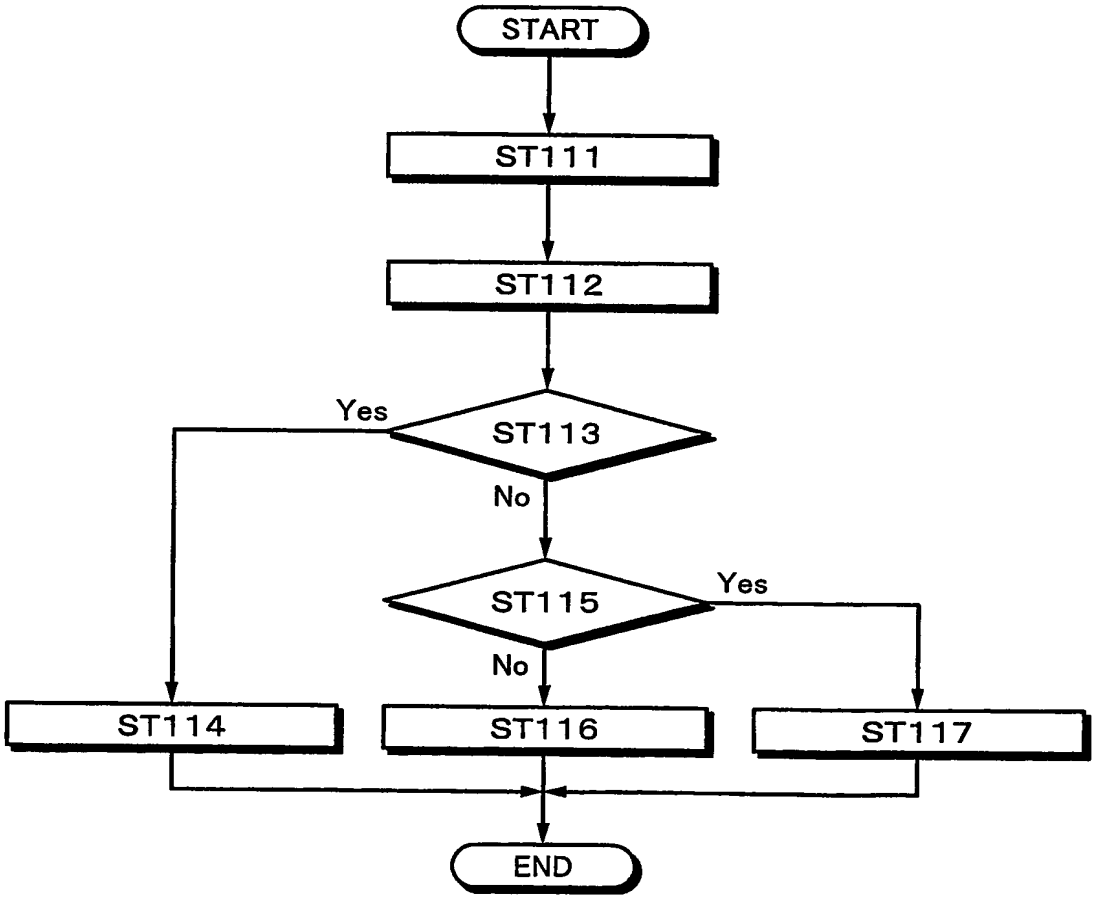
第２８図


92
PC
認証キー
Km
RNG
404
MAC
406
CMP
410
DEMUX
401
ディスク タイプ
301
RNG
405
MAC
407
RNG
409
Ksを生成
408
セッションキー=Ks=eKm(Ra3 || Rb3)
128ビット
Rb1
64ビット
eKm(Ra1 || Rb1)
128ビット
Ra1
64ビット
Rb2
64ビット
eKm(Rb2 || Ra2)
128ビット
Ra2
64ビット
Rb3
64ビット
Ra3
64ビット
91
ドライブ
認証キー
Km
MAC
306
CMP
310
MAC
307
Ksを生成
308
セッションキー=Ks=eKm(Ra3 || Rb3)
128ビット
RNG
309
301
ディスク タイプ
(0,0):ROM
(0,1):リザーブド
(1,0):ライタブル タイプ1
(1,1):ライタブル タイプ2
MUX
302
MUX
303
RNG
304
ディスク タイプ
301
RNG
305

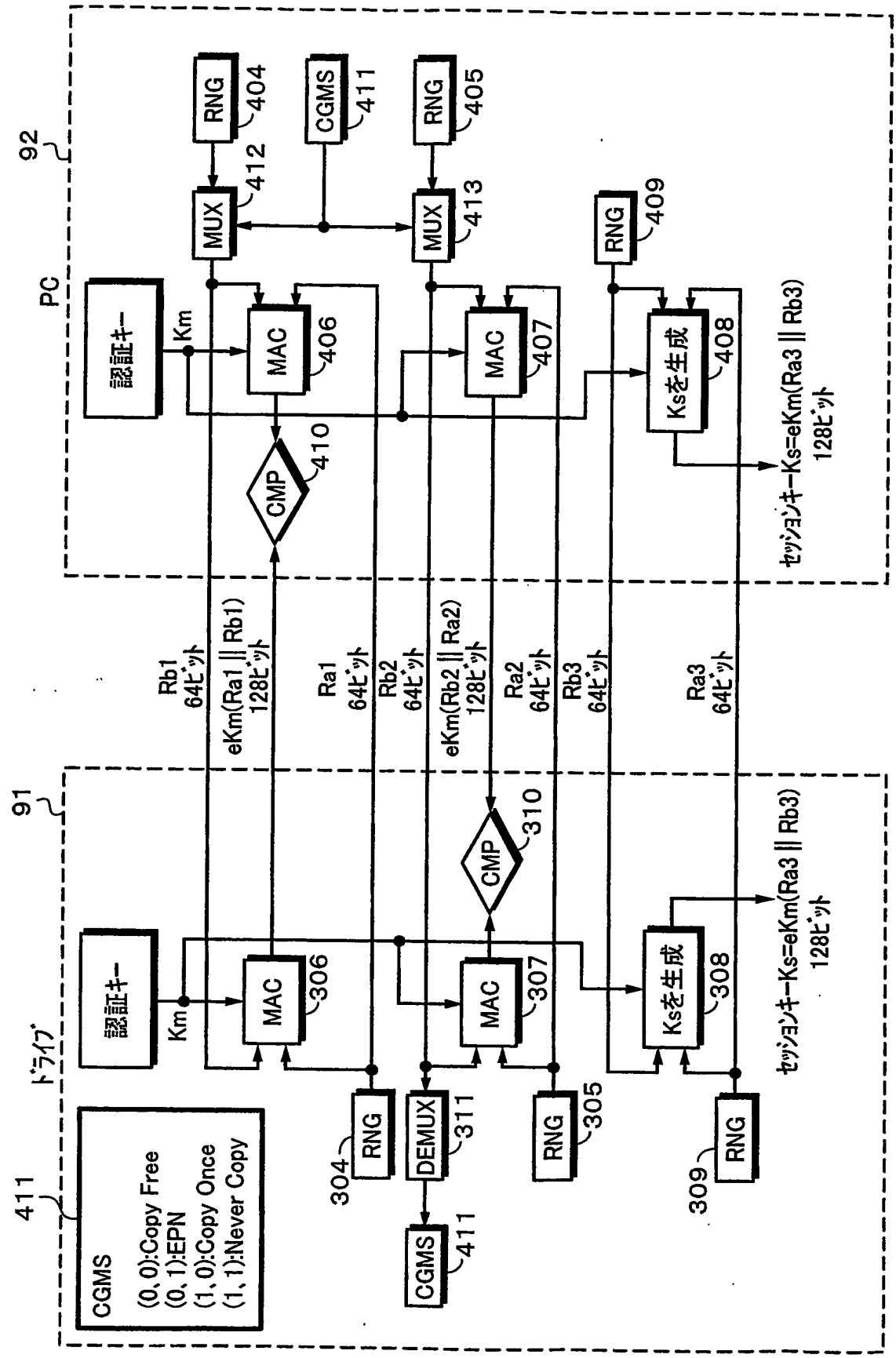
第２９図



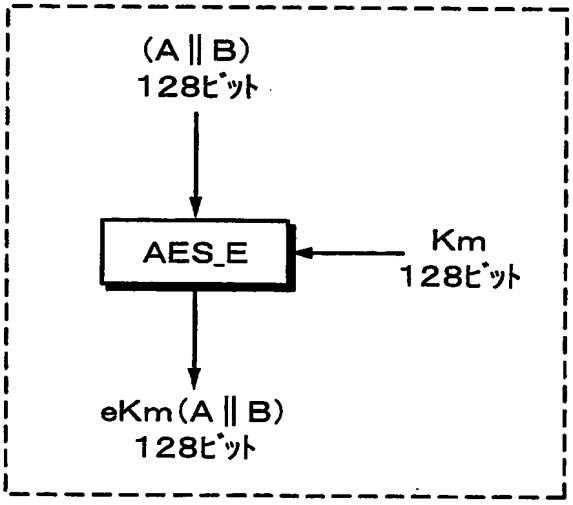
第３０図


START
ST111
ST112
ST113
Yes
No
ST115
Yes
No
ST114
ST116
ST117
END

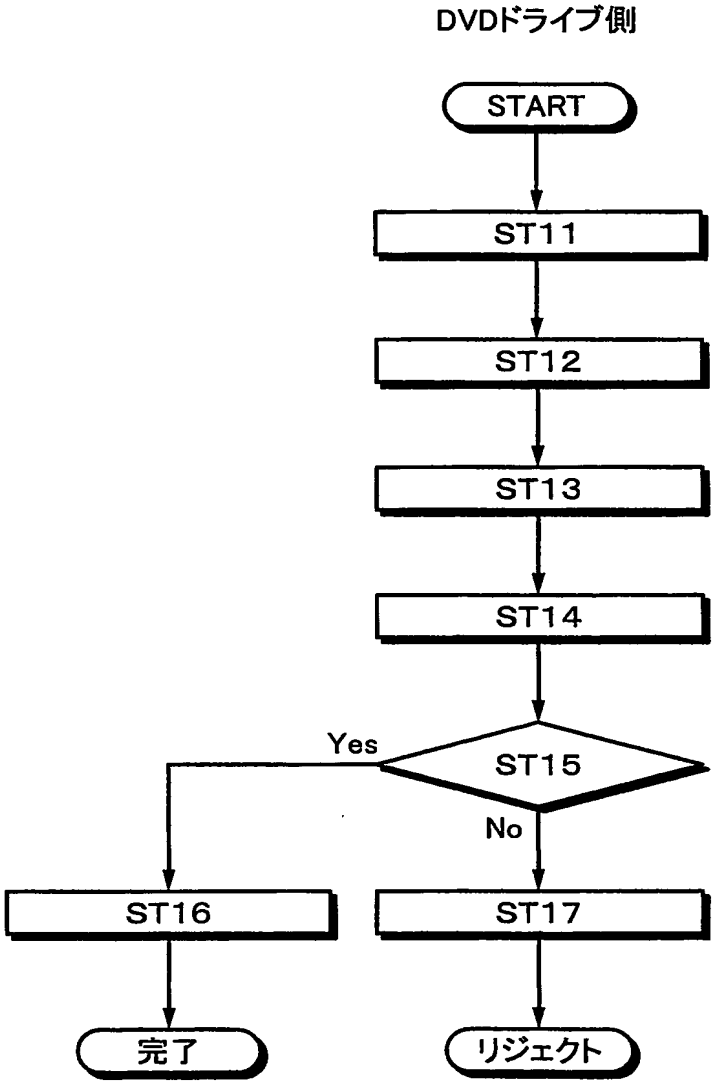
第３１図


92
PC
RNG
404
CGMS
411
RNG
405
MUX
412
MUX
413
RNG
409
認証キー
Km
MAC
406
MAC
407
Ksを生成
408
CMP
410
セッションキー=Ks=eKm(Ra3 || Rb3)
128ビット
Rb1
64ビット
eKm(Ra1 || Rb1)
128ビット
Ra1
64ビット
Rb2
64ビット
eKm(Rb2 || Ra2)
128ビット
Ra2
64ビット
Rb3
64ビット
Ra3
64ビット
91
CMP
310
認証キー
Km
MAC
306
MAC
307
Ksを生成
308
セッションキー=Ks=eKm(Ra3 || Rb3)
128ビット
ドライブ
411
CGMS
(0,0):Copy Free
(0,1):EPN
(1,0):Copy Once
(1,1):Never Copy
304
RNG
DEMUX
311
RNG
305
309
RNG
CGMS
411

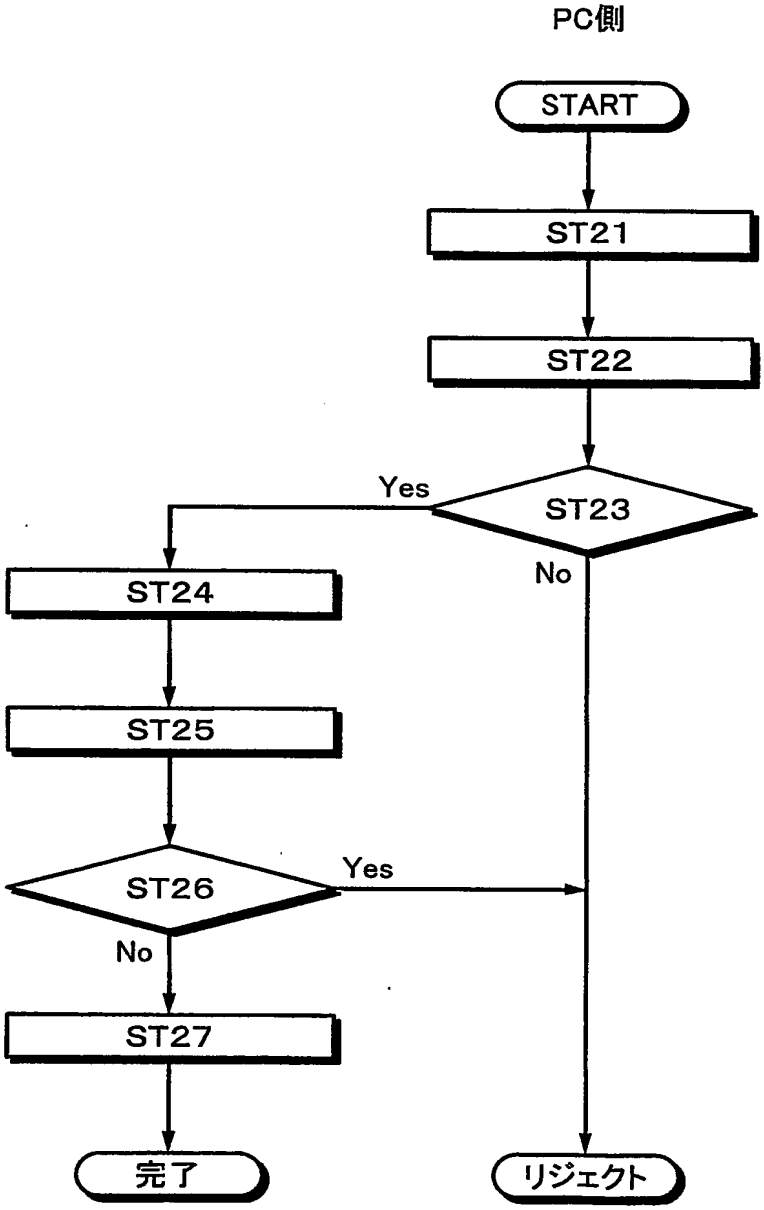
第３２図



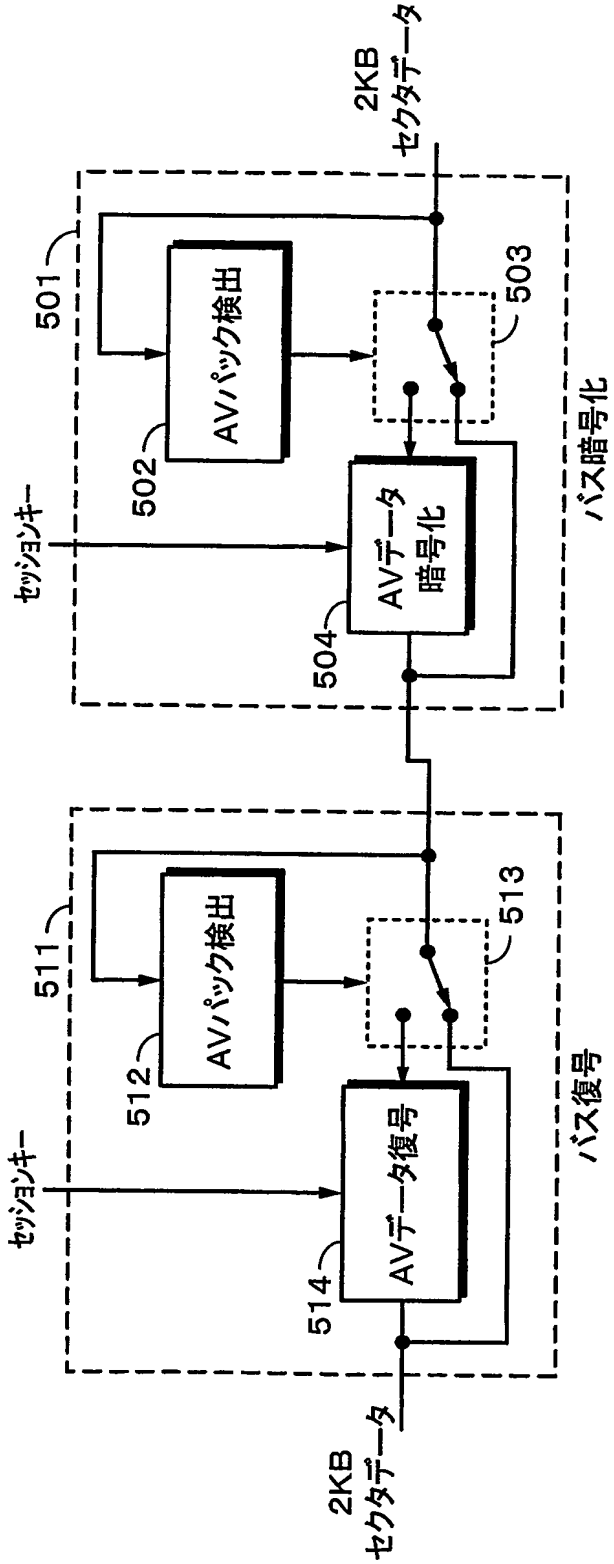
第３３図


DVDドライブ側
START
ST11
ST12
ST13
ST14
ST15
Yes
No
ST16
ST17
完了
リジェクト

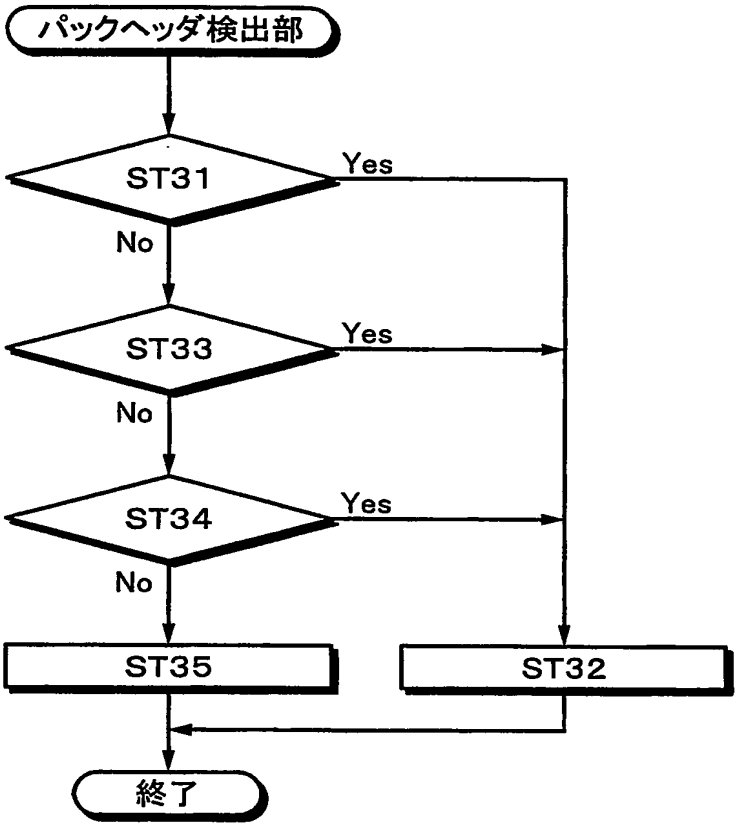
第３４図


PC側
START
ST21
ST22
ST23
Yes
No
ST24
ST25
ST26
Yes
No
ST27
完了
リジェクト

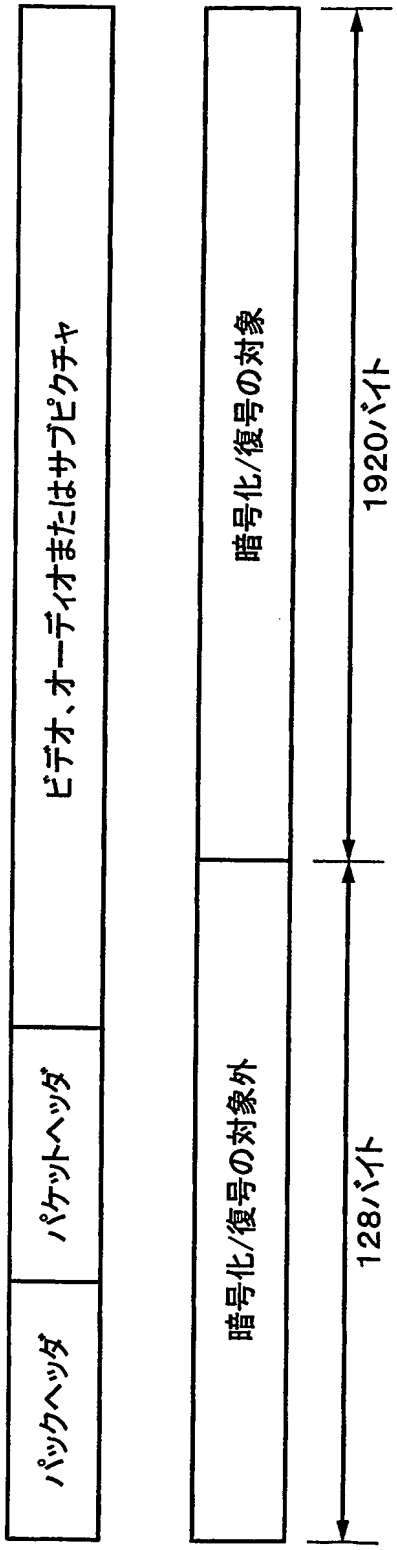
第35図


2KB
セクタデータ
501
AVパック検出
502
503
セッションキー
AVデータ
暗号化
504
バス暗号化
511
AVパック検出
512
513
セッションキー
AVデータ復号
514
バス復号
2KB
セクタデータ

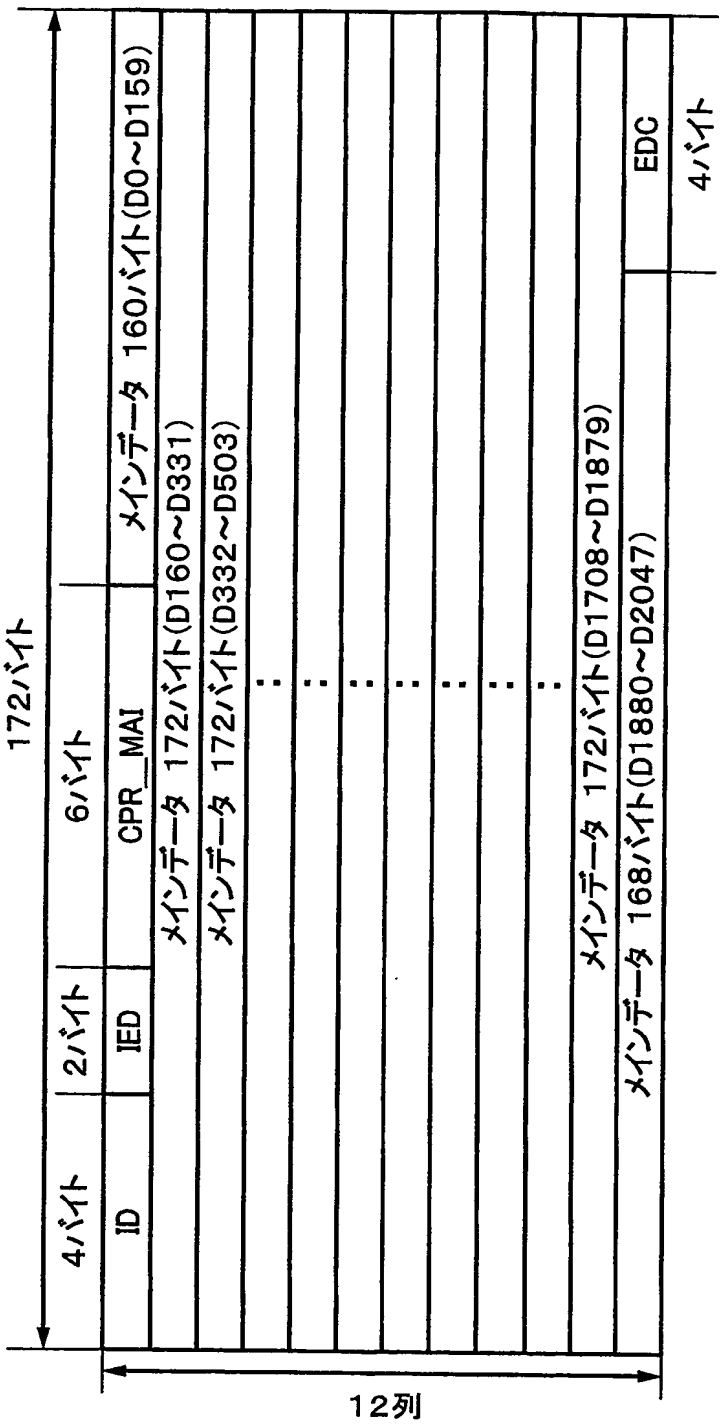
第３６図



第３７図

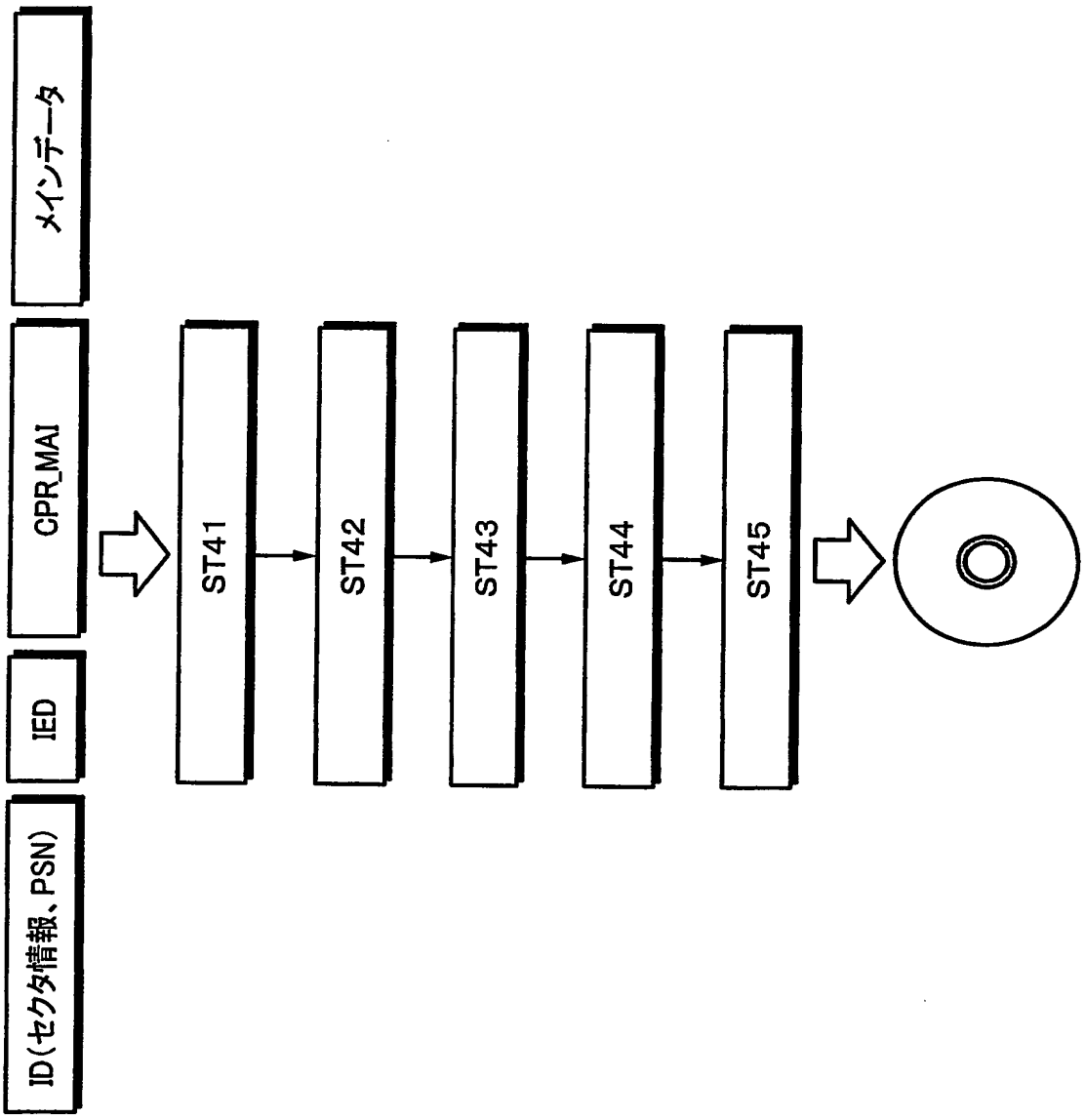

パックヘッダ
パケットヘッダ
ビデオ、オーディオまたはサブピクチャ
暗号化/復号の対象外
暗号化/復号の対象
128バイト
1920バイト

第３８図

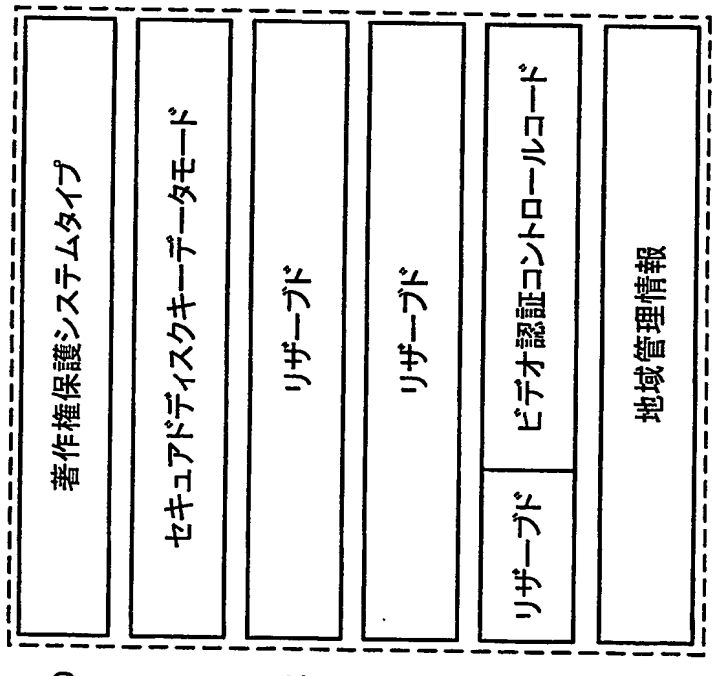

172バイト
4バイト
2バイト
6バイト
ID
IED
CPR_MAI
メインデータ 160バイト(D0~D159)
メインデータ 172バイト(D160~D331)
メインデータ 172バイト(D332~D503)
メインデータ 172バイト(D1708~D1879)
メインデータ 168バイト(D1880~D2047)
EDC
4バイト
12列

セクタ構成例

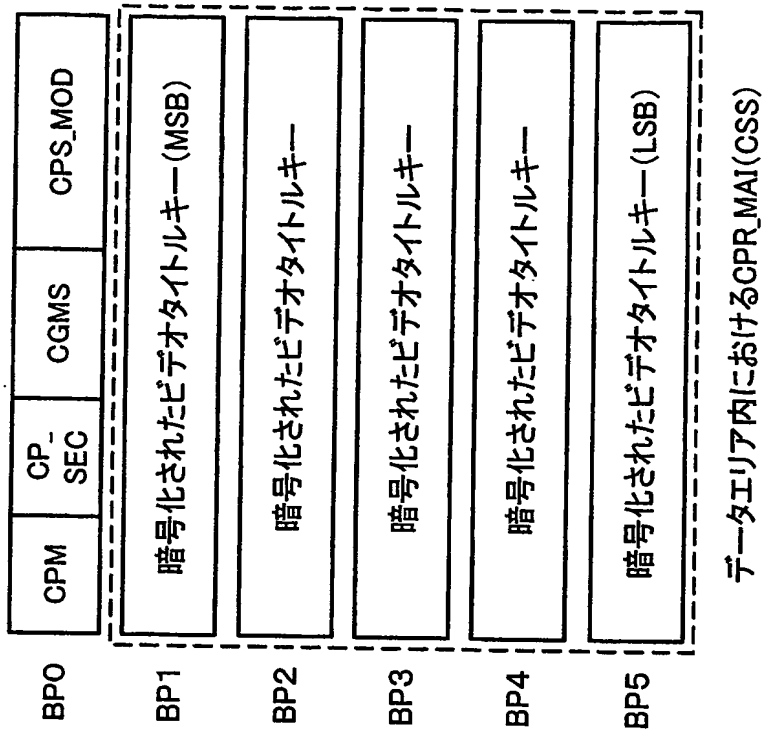
第３９図



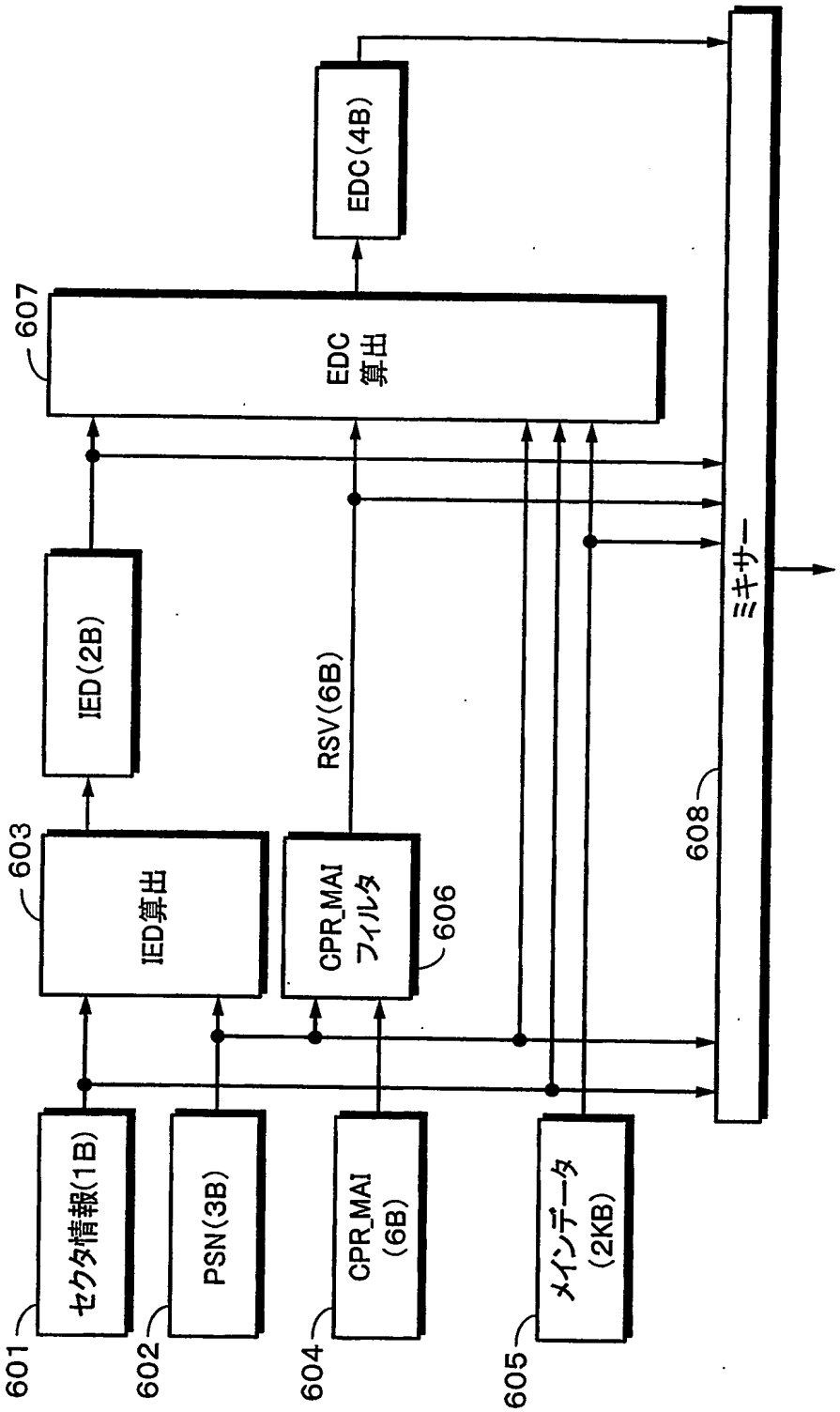
第４０図Ａ


著作権保護システムタイプ
セキュアドディスクキーデータモード
リザーブド
リザーブド
リザーブド
ビデオ認証コントロールコード
地域管理情報
BP0
BP1
BP2
BP3
BP4
BP5
リードインエリア内におけるCPR_MAI
… マスキングエリア

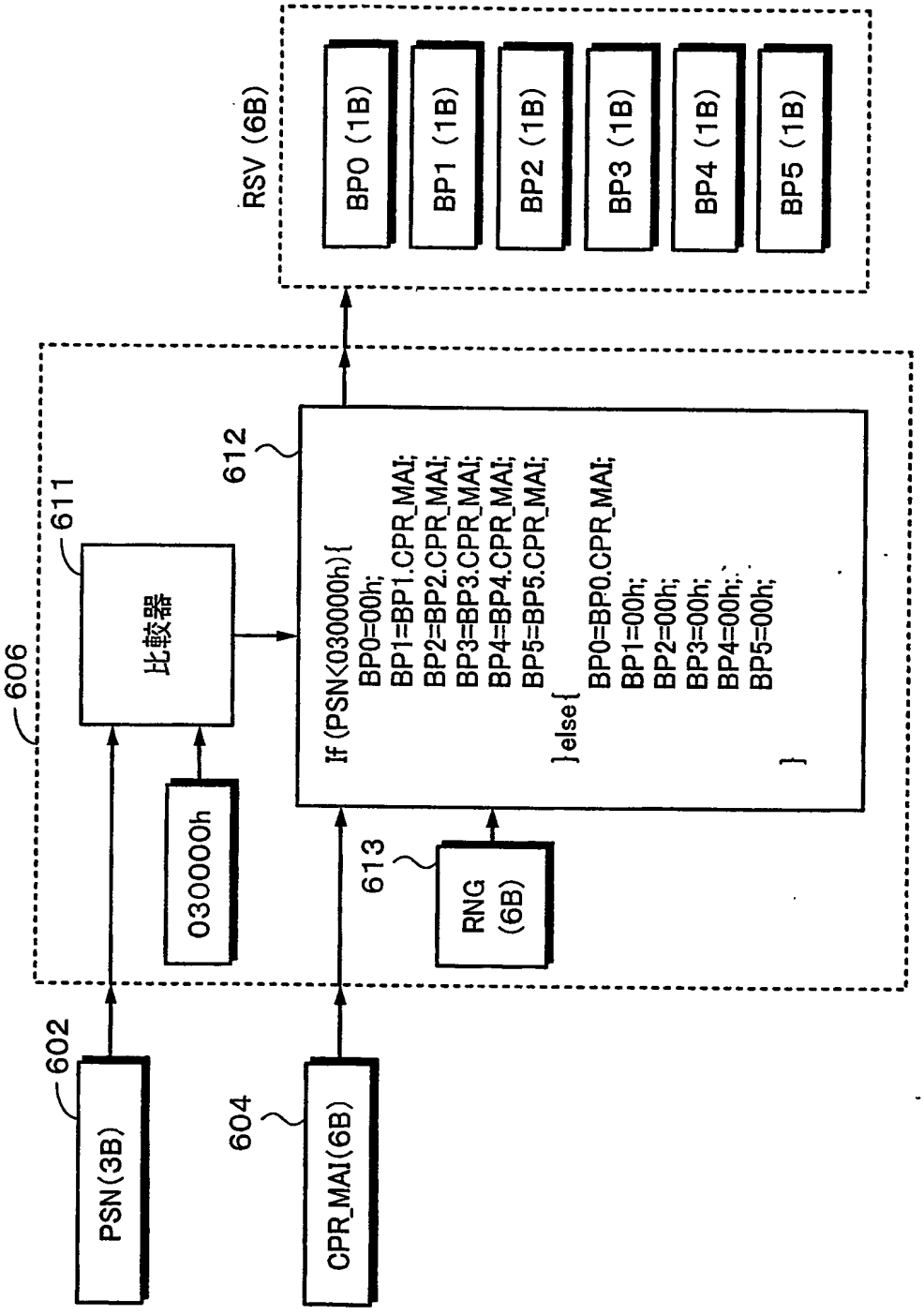
第４０図Ｂ


CPM
CP_SEC
CGMS
CPS_MOD
暗号化されたビデオタイトルキー(MSB)
暗号化されたビデオタイトルキー
暗号化されたビデオタイトルキー
暗号化されたビデオタイトルキー
暗号化されたビデオタイトルキー(LSB)
BP0
BP1
BP2
BP3
BP4
BP5
データエリア内におけるCPR_MAI(CSS)

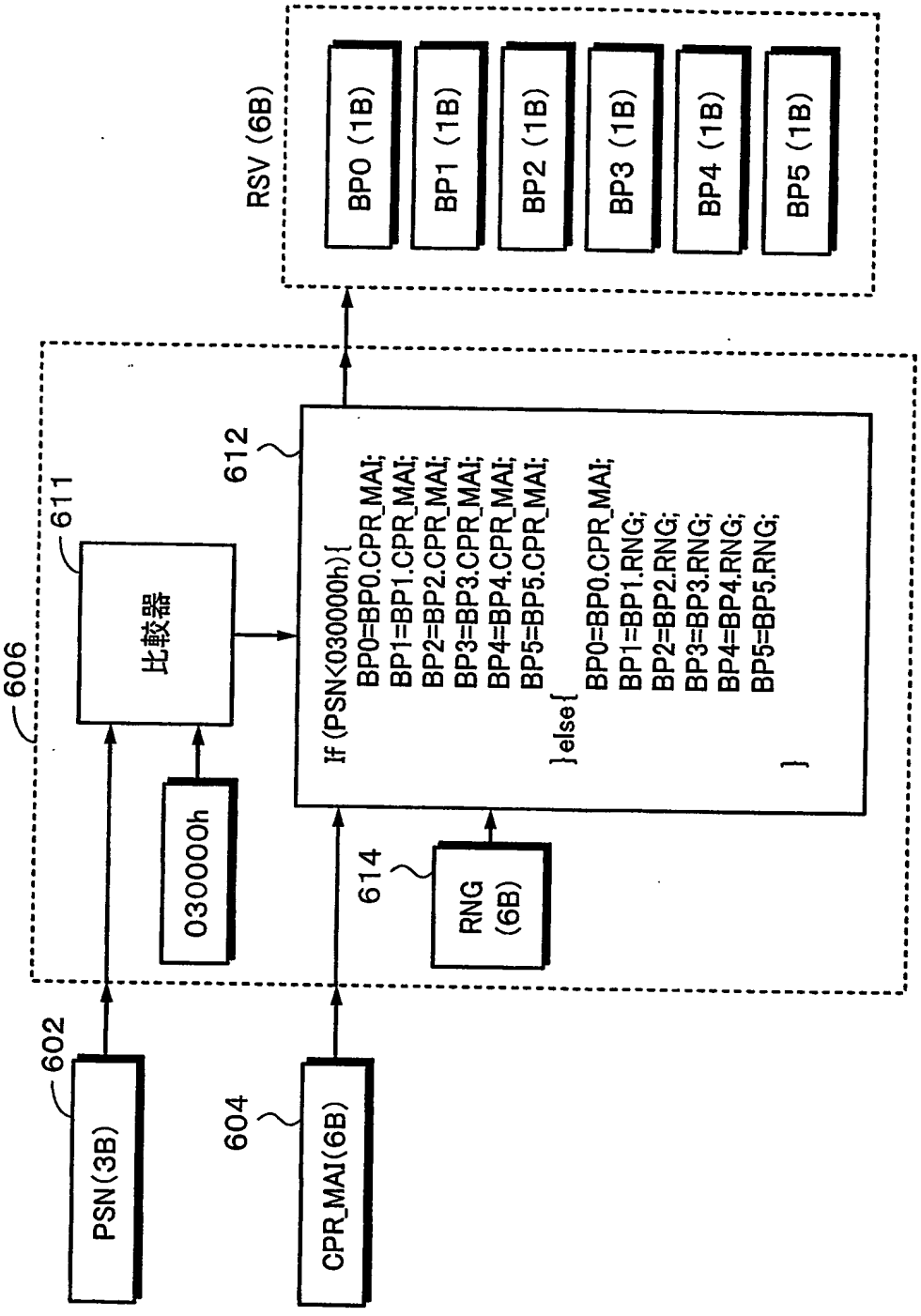
第４１図


セクタ情報(1B)
PSN(3B)
CPR_MAI (6B)
メインデータ (2KB)
IED算出
CPR_MAI フィルタ
IED(2B)
RSV(6B)
EDC 算出
EDC(4B)
ミキサー
601
602
603
604
605
606
607
608

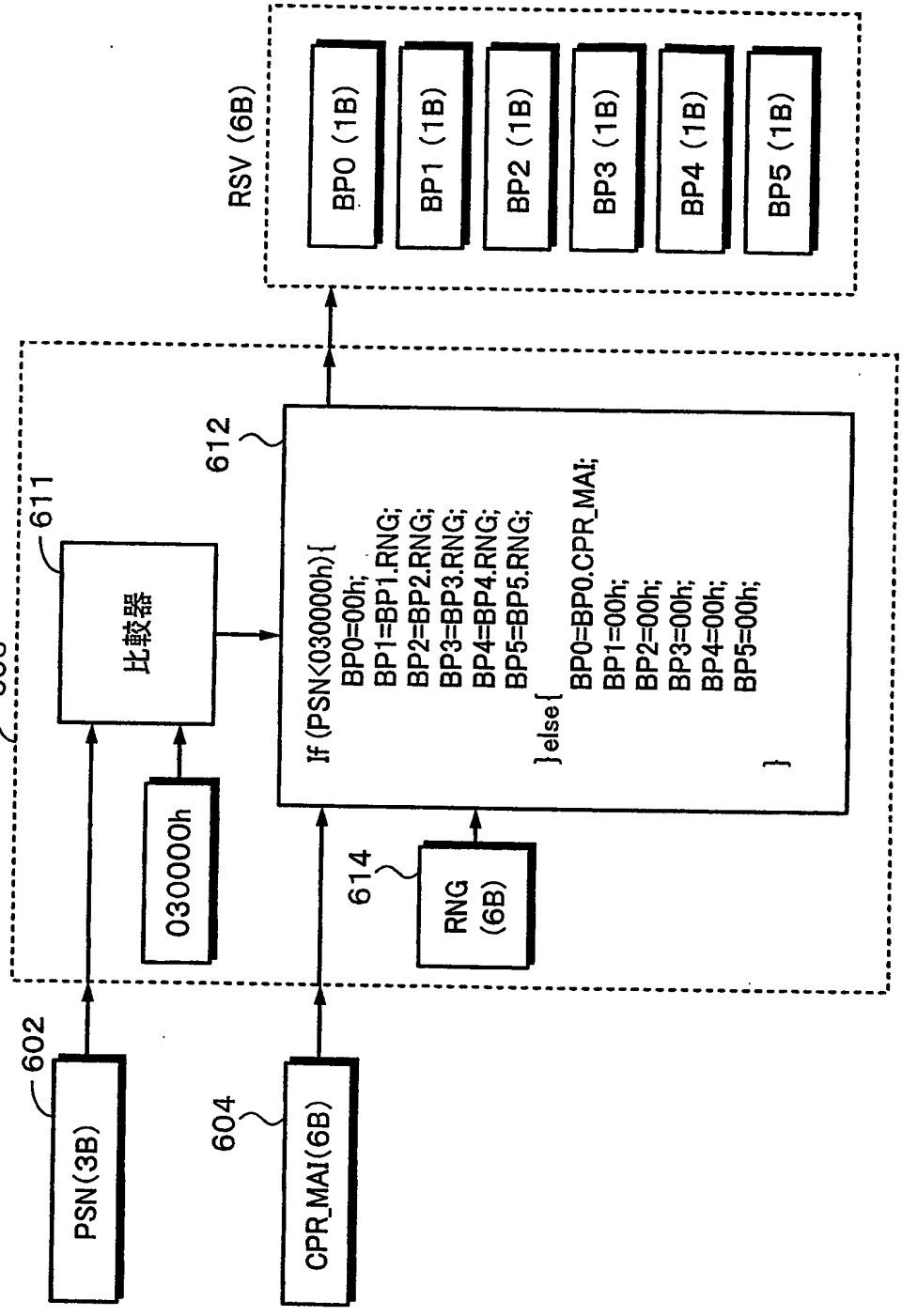
第４２図


RSV (6B)
BP0 (1B)
BP1 (1B)
BP2 (1B)
BP3 (1B)
BP4 (1B)
BP5 (1B)
606
611
比較器
612
If (PSN<030000h){
BP0=00h;
BP1=BP1.CPR_MAI;
BP2=BP2.CPR_MAI;
BP3=BP3.CPR_MAI;
BP4=BP4.CPR_MAI;
BP5=BP5.CPR_MAI;
}else{
BP0=BP0.CPR_MAI;
BP1=00h;
BP2=00h;
BP3=00h;
BP4=00h;
BP5=00h;
}
030000h
613
RNG (6B)
602
PSN(3B)
604
CPR_MAI(6B)

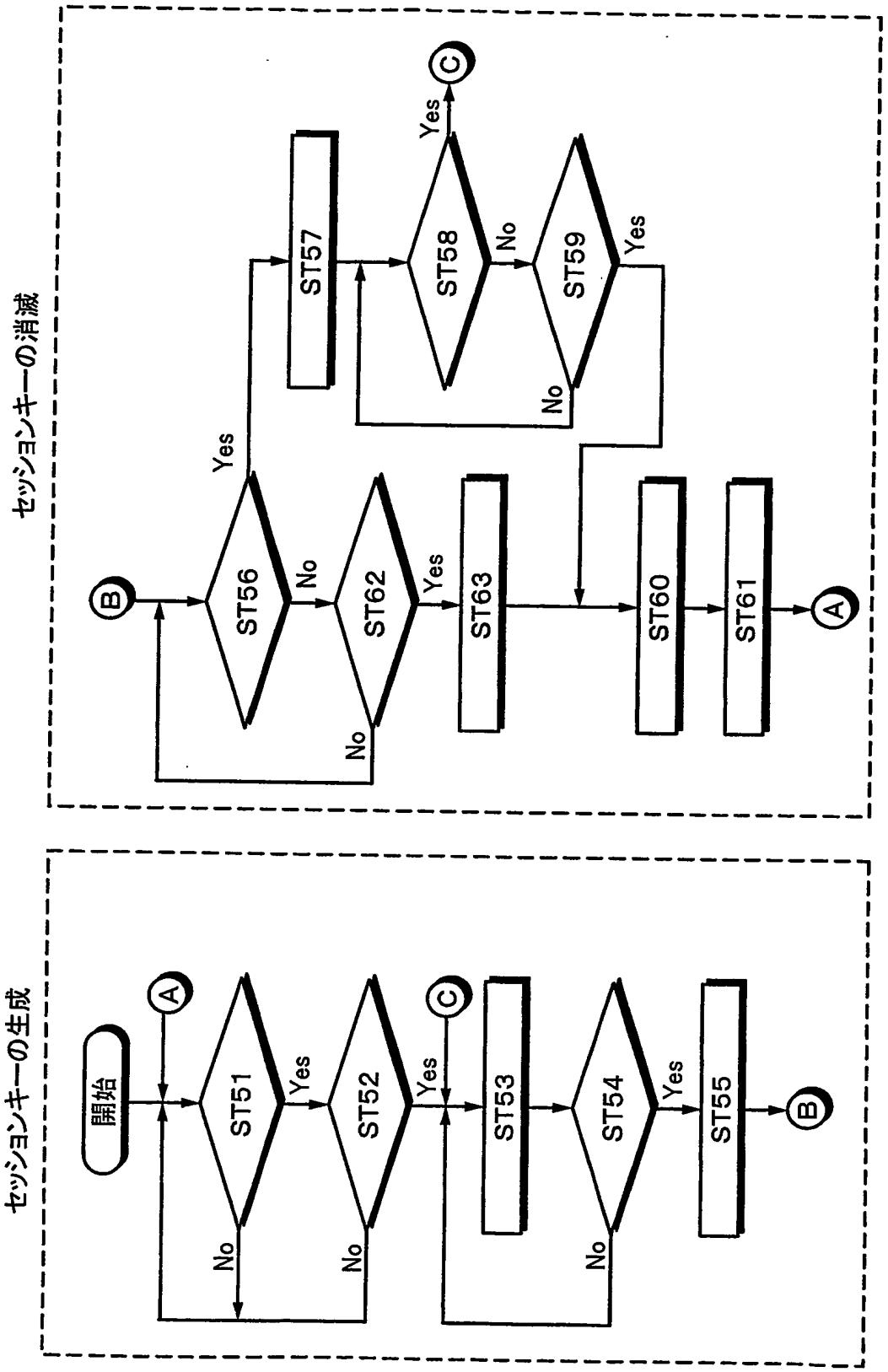
第４３図


RSV (6B)
BP0 (1B)
BP1 (1B)
BP2 (1B)
BP3 (1B)
BP4 (1B)
BP5 (1B)
606
611
比較器
612
If (PSN<030000h){
BP0=BP0.CPR_MAI;
BP1=BP1.CPR_MAI;
BP2=BP2.CPR_MAI;
BP3=BP3.CPR_MAI;
BP4=BP4.CPR_MAI;
BP5=BP5.CPR_MAI;
}else{
BP0=BP0.CPR_MAI;
BP1=BP1.RNG;
BP2=BP2.RNG;
BP3=BP3.RNG;
BP4=BP4.RNG;
BP5=BP5.RNG;
}
030000h
614
RNG (6B)
602
PSN(3B)
604
CPR_MAI(6B)

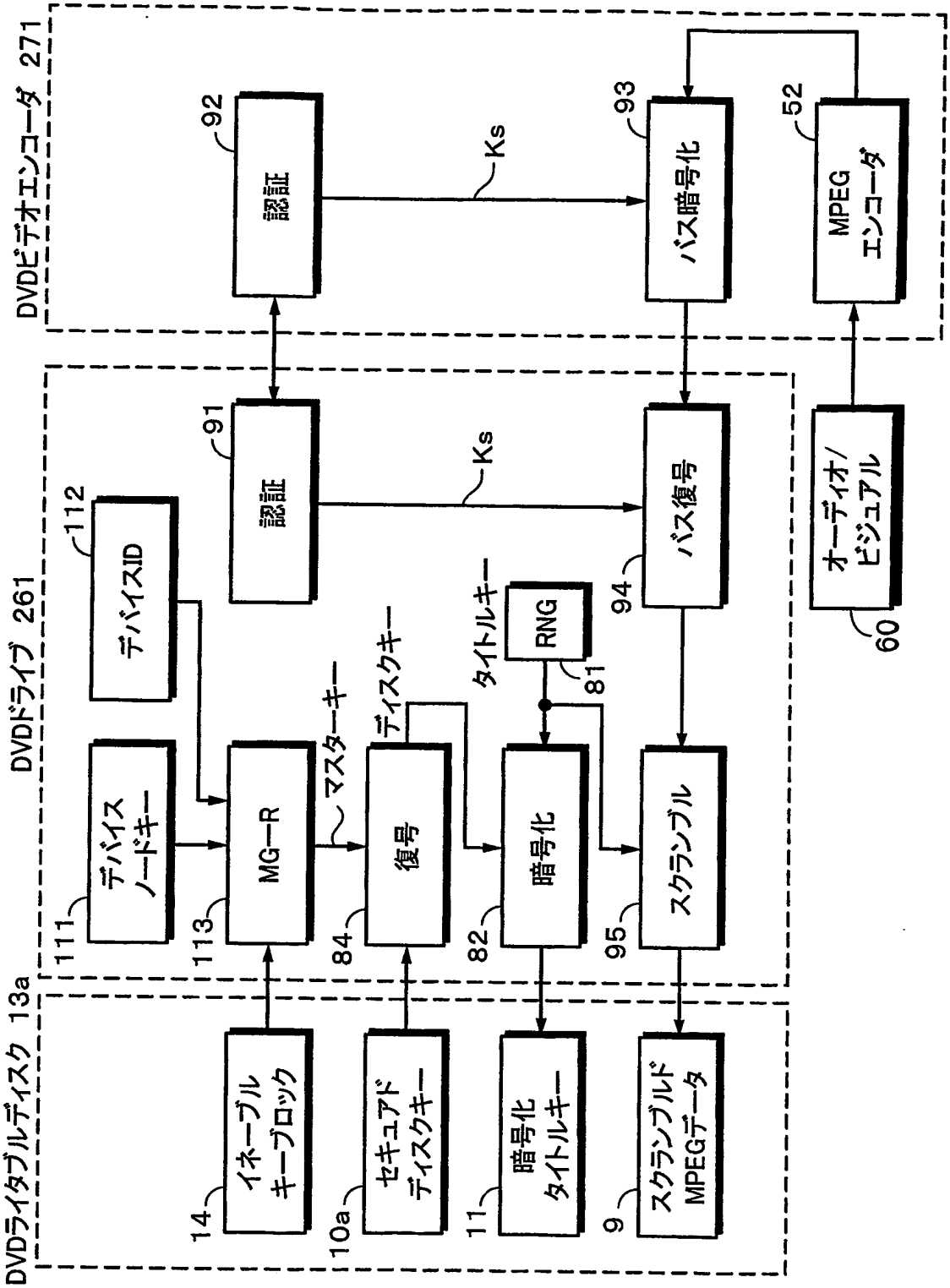
第44図


RSV (6B)
BP0 (1B)
BP1 (1B)
BP2 (1B)
BP3 (1B)
BP4 (1B)
BP5 (1B)
612
611
606
比較器
030000h
614
RNG (6B)
602
PSN(3B)
604
CPR_MAI(6B)
If (PSN<030000h){
BP0=00h;
BP1=BP1.RNG;
BP2=BP2.RNG;
BP3=BP3.RNG;
BP4=BP4.RNG;
BP5=BP5.RNG;
}else{
BP0=BP0.CPR_MAI;
BP1=00h;
BP2=00h;
BP3=00h;
BP4=00h;
BP5=00h;
}

第４５図


セッションキーの生成
開始
A
ST51
Yes
No
ST52
Yes
No
C
ST53
ST54
Yes
No
ST55
B
セッションキーの消滅
B
ST56
Yes
No
ST62
Yes
No
ST63
ST57
C
Yes
ST58
No
ST59
Yes
No
ST60
ST61
A

第４６図


DVDビデオエンコーダ 271
92
認証
Ks
93
バス暗号化
52
MPEG
エンコーダ
DVDドライブ 261
91
認証
Ks
バス復号
94
オーディオ/
ビジュアル
60
112
デバイスID
タイトルキー
RNG
81
ディスクキー
マスターキー
デバイス
ノードキー
MG−R
復号
暗号化
スクランブル
111
113
84
82
95
DVDライタブルディスク 13a
イネーブル
キーブロック
セキュアド
ディスクキー
暗号化
タイトルキー
スクランブルド
MPEGデータ
14
10a
11
9

符号の説明

ＳＴ１０１　メディアタイプ判別
ＳＴ１０２　ＲＯＭ？
ＳＴ１０３　ディスクタイプ＝ＲＯＭ
ＳＴ１０４　ディスクアプリケーションコード＝ビデオライタブル？
ＳＴ１０５　ディスクタイプ＝リザーブド
ＳＴ１０６　ディスクタイプ＝ビデオライタブル

ＳＴ１１１　相互認証
ＳＴ１１２　ディスクタイプをドライブから取得
ＳＴ１１３　ディスクタイプ＝ＲＯＭ？
ＳＴ１１４　データ書き込み禁止
ＳＴ１１５　ディスクタイプ＝ビデオライタブル？
ＳＴ１１６　データ書き込み可能
ＳＴ１１７　ＣＳＳ／ＣＰＲＭビデオ書き込み可能

ＳＴ１１　ＲＥＣＥＩＶＥ（Ｒｂ１，Ｒｂ２）
ＳＴ１２　ＲＥＴＵＲＮ（ｅＫｍ（Ｒａ１‖Ｒｂ１），Ｒａ１）
ＳＴ１３　ＲＥＴＵＲＮ（Ｒａ２，Ｒａ３）
ＳＴ１４　ＲＥＣＥＩＶＥ（ｅＫｍ（Ｒｂ２‖Ｒａ２），Ｒｂ３）
ＳＴ１５　同一のＭＡＣ？
ＳＴ１６　セッションキーの確定（ｅＫｍ（Ｒａ３‖Ｒｂ３）
ＳＴ１７　ＲＥＴＵＲＮ（エラー）

ＳＴ２１　ＳＥＮＤ　ＫＥＹ（Ｒｂ１，Ｒｂ２）

ＳＴ２２　ＲＥＰＯＲＴ　ＫＥＹ（ｅＫｍ（Ｒａ１‖Ｒｂ１），Ｒａ１）

ＳＴ２３　同一のＭＡＣ？

ＳＴ２４　ＲＥＰＯＲＴ　ＫＥＹ（Ｒａ２，Ｒａ３）

ＳＴ２５　ＳＥＮＤ　ＫＥＹ（ｅＫｍ（Ｒｂ２‖Ｒａ２），Ｒｂ３）

ＳＴ２６　エラー？

ＳＴ２７　セッションキーの確定（ｅＫｍ（Ｒａ３‖Ｒｂ３）

ＳＴ３１　ビデオパック

ＳＴ３２　データを暗号化／復号する

ＳＴ３３　オーディオパック

ＳＴ３４　サブピクチャパック

ＳＴ３５　データを暗号化／復号しない

ＳＴ４１　ＥＤＣを加える

ＳＴ４２　スクランブルメインデータ

ＳＴ４３　ＥＣＣの符号化

ＳＴ４４　ＰＯを１６列インターリーブ

ＳＴ４５　セクタ毎に２６シンクフレーム変調

ＳＴ５１　ＤＶＤ＋ＲＷ／＋Ｒディスク挿入？

ＳＴ５２　ＰＣアプリケーション起動？

ＳＴ５３　相互認証し、セッションキーを生成

ＳＴ５４　完了した？

ＳＴ５５　ＣＳＳキー書き込み禁止を解除

ＳＴ５６　ＰＣアプリケーション終了？

ＳＴ５７　ＰＣ内で生成したセッションキーを消去

ＳＴ５８　ＰＣアプリケーション起動？

ＳＴ５９　ＤＶＤ＋ＲＷ／＋Ｒディスク排出？

ＳＴ６０　ドライブ内で生成したセッションキーを消去

ＳＴ６１　ＣＳＳキー書き込み禁止

９	スクランブルドＭＰＥＧデータ
１０ａ，１０ｂ	セキュアドディスクキー
１１	暗号化タイトルキー
１３ａ，１３ｂ	ライタブルディスク
５２	ＭＰＥＧエンコーダ
５３，９５	スクランブラ
５６，７８，８４	デクリプタ
５７，８３	マスターキー
６０	オーディオ／ビジュアルデータ
６２，７２	認証部
６３，７６，８５	バスエンクリプタ
６６，７３，７７	バスデクリプタ
８１，８６	乱数発生器
８２，８７	エンクリプタ
１０１，１０２	マスクコントロール
１６１，２６１	ドライブ
１７１，２７１	ＰＣ

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2004/013980

A. CLASSIFICATION OF SUBJECT MATTER
Int.Cl[7] H04L9/08, H04L12/14, G11B20/10

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
Int.Cl[7] H04L9/08, H04L12/14, G11B20/10

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Jitsuyo Shinan Koho	1922-1996	Toroku Jitsuyo Shinan Koho	1994-2004
Kokai Jitsuyo Shinan Koho	1971-2004	Jitsuyo Shinan Toroku Koho	1996-2004

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	JP 2001-331106 A (Matsushita Electric Industrial Co., Ltd.), 30 November, 2001 (30.11.01), Figs. 2 to 15; Par. Nos. [0076] to [0093]	1-4,9-12, 17-19,23-25, 29-32,37-40, 45,47,49,51
Y	& EP 1134964 A2	5-8,13-16, 20-22,26-28, 33-36,41-44, 46,48,50,52

[X] Further documents are listed in the continuation of Box C. [ ] See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search 08 December, 2004 (08.12.04)	Date of mailing of the international search report 21 December, 2004 (21.12.04)
Name and mailing address of the ISA/ Japanese Patent Office Facsimile No.	Authorized officer Telephone No.

Form PCT/ISA/210 (second sheet) (January 2004)

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2004/013980

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	JP 10-210025 A (Matsushita Electric Industrial Co., Ltd.), 07 August, 1998 (07.08.98), Fig. 6; Par. Nos. [0056] to [0065] & EP 840476 A2	5-8,13-16, 20-22,26-28, 33-36,41-44, 46,48,50,52
A	JP 2001-77802 A (Sony Corp.), 23 March, 2001 (23.03.01), Full text (Family: none)	1-52
A	JP 2001-236729 A (Hitachi, Ltd.), 31 August, 2001 (31.08.01), Figs. 5, 7; Par. Nos. [0024] to [0041] & EP 951019 A2	1-52
A	JP 2002-353960 A (Fujitsu Ltd.), 06 December, 2002 (06.12.02), Fig. 10; Par. Nos. [0046] to [0049] & EP 1278114 A2	1-52

国際調査報告

国際出願番号　PCT／JP2004／013980

A.　発明の属する分野の分類（国際特許分類（IPC））

Int. Cl⁷　H04L9／08, H04L12／14, G11B20／10

B.　調査を行った分野

調査を行った最小限資料（国際特許分類（IPC））

Int. Cl⁷　H04L9／08, H04L12／14, G11B20／10

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報　1922－1996年
日本国公開実用新案公報　1971－2004年
日本国登録実用新案公報　1994－2004年
日本国実用新案登録公報　1996－2004年

国際調査で使用した電子データベース（データベースの名称、調査に使用した用語）

C.　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
X	JP 2001－331106 A（松下電器産業株式会社）2001.11.30, 第2－15図, 【0076】－【0093】段落 & EP 1134964 A2	1-4, 9-12, 17-19, 23-25, 29-32, 37-40, 45, 47, 49, 51
Y		5-8, 13-16, 20-22, 26-28, 33-36, 41-44, 46, 48, 50, 52

☒ C欄の続きにも文献が列挙されている。　☐ パテントファミリーに関する別紙を参照。

＊　引用文献のカテゴリー
「A」特に関連のある文献ではなく、一般的技術水準を示すもの
「E」国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの
「L」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献（理由を付す）
「O」口頭による開示、使用、展示等に言及する文献
「P」国際出願日前で、かつ優先権の主張の基礎となる出願の日の後に公表された文献
「T」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの
「X」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの
「Y」特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの
「&」同一パテントファミリー文献

国際調査を完了した日	国際調査報告の発送日
08.12.2004	21.12.2004

国際調査機関の名称及びあて先
日本国特許庁（ISA／JP）
郵便番号100－8915
東京都千代田区霞が関三丁目4番3号

特許庁審査官（権限のある職員）　5M　9469
石田　信行

電話番号　03－3581－1101　内線　3598

C（続き）．　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
Y	JP 10－210025 A（松下電器産業株式会社） 1998．08．07，第6図，【0056】－【0065】段落 ＆ EP 840476 A2	5-8, 13-16, 20-22, 26-28, 33-36, 41-44, 46, 48, 50, 52
A	JP 2001－77802 A（ソニー株式会社） 2001．03．23，全文（ファミリーなし）	1 - 52
A	JP 2001－236729 A（株式会社日立製作所） 2001．08．31， 第5，7図，【0024】－【0041】段落 ＆ EP 951019 A2	1 - 52
A	JP 2002－353960 A（富士通株式会社） 2002．12．06， 第10図，【0046】－【0049】段落 ＆ EP 1278114 A2	1 - 52